BACHELOR'S THESIS

Degree in Mathematics

Title: The Kronecker-Weber Theorem

Author: Damià Fulton Arrufat

Advisor: Jordi Quer Bosor

Department: Algebraic Number Theory

Academic year: 2017-2018

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Contents

Introduction

In Galois Theory (the study of field extensions and their corresponding group of field automorphisms) one of the easiest cases to study is when we adjoin a primitive n-th root of unity (which we will denote by ζ_n) to our base field. We call these *cyclotomic extensions*. We will show in chapter 1 that for any field K, the Galois group of $K(\zeta_n)$ over K is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. In fact, when $K = \mathbb{Q}$, we have an isomorphism for every $n \geq 1$.

With a little Galois and group theory, using this result we can prove that for any finite abelian group A, there will exist infinitely many finite extensions $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong A$. These fields are constructed as subextensions of cyclotomic extensions of $\mathbb{Q}$, that is $K \subseteq \mathbb{Q}(\zeta_n)$ for some $n \geq 1$.

The Kronecker-Weber theorem says that this is the only way: it states that every finite extension K over $\mathbb{Q}$ with abelian Galois group is contained in some cyclotomic extension of $\mathbb{Q}$.

So not only do we have a way to construct abelian extensions (taking subfields of cyclotomic extensions) but with this method we get EVERY abelian extension of $\mathbb{Q}$.

The aim of this thesis is to present a complete proof of the Kronecker-Weber theorem, together with the necessary theory for doing this.

The theorem was first stated by L. Kronecker in 1853, but he failed to prove the case when the extension has degree a power of 2. In 1886, H. Weber gave another proof, which was later shown to also have a gap in it. It was finally D. Hilbert who was able to give the first complete proof of the theorem using ramification groups, in 1896. The theorem is named after the first two mathematicians.

The Kronecker-Weber theorem is not true for number fields in general: that is, not all abelian extensions of a number field lie in some cyclotomic extension of it. In 1900, Hilbert included a generalization of the Kroneceker-Weber theorem in his list of 23 unresolved problems. It is known as Hilbert's 12-th problem, and its aim is to find, for a given number field K, analogues of the roots of unity such that when adjoined to K, they generate every finite abelian extension of K. This question is still unresolved in general. Only the case of imaginary quadratic fields has been solved, in the theory of complex multiplication, using elliptic and modular functions. For a very interesting historic note on Hilbert's 12-th problem and its first developments see [Sch98].

A modern approach to prove the Kronecker-Weber theorem is to show it as a consequence of class field theory. There are also more elementary proofs, such as M. Greenberg's [Gre74], following Hilbert's use of ramification theory.

Our approach will be based on a local-global principle, following a modification of I. Safarevich's proof by L. Washington. In other words, we will prove that the (global) Kronecker-Weber theorem holds for $\mathbb{Q}$ if and only if it holds for $\mathbb{Q}_p$, for every prime p, and then we will prove this local version of the theorem.

Here $\mathbb{Q}_p$ denotes the field of p-adic numbers, the completion of $\mathbb{Q}$ with respect to an absolute value related to the prime p, the p-adic absolute value. As a matter of fact, these fields together with $\mathbb{R}$ are all the possible completions of $\mathbb{Q}$ with respect to some absolute value. The field of p-adic numbers was first introduced by K. Hensel in the beginning of the 20 th century. It is a very powerful mathematical tool, since it is used to solve many arithmetic problems by local-global principles: properties that are true for $\mathbb{Q}$ if and only if they are true for $\mathbb{R}$ and $\mathbb{Q}_p$ for all p. In this sense, the Kronecker-Weber theorem is an example of this kind of principle, but it doesn't work in general.

We will begin by explaining some concepts of number theory and local fields that will be the backbone of our thesis. In chapter 2 we construct and discuss the nature of the p-adic numbers. Then we develop the most important results on its finite extensions and ramification theory in chapter 3. Chapter 4 is a short digression on cyclotomic extensions and Kummer theory, which we will make use of in the proof of the theorem. Finally, chapter 5 contains the actual proof of the local-global principle as well as the proof of the local Kronecker-Weber theorem, and thus proving the global version of it.

I would like to thank my advisor, professor Jordi Quer, for his patience and advice during the elaboration of this Bachelor's Thesis.

1 Introductory Concepts

In this first chapter we introduce some concepts of algebraic number theory and group theory that we need in order to study the p-adic numbers and for the proof of the Kronecker-Weber theorem. We finish the chapter by showing the results that motivate the theorem.

1.1 Valuations and Local Fields

For this first section we are following the first chapter in [Ser79].

Definition 1.1. *A ring A is said to be **local** if it has exactly one maximal ideal.*

Definition 1.2. *A principal ideal domain which is also a local ring with a non-zero maximal ideal is called a **discrete valuation ring** (D.V.R.). In this case, the ring has exactly one non-zero prime ideal, namely the non-zero maximal ideal. We denote it by $\mathfrak{p}$.*

If A is a discrete valuation ring, with prime ideal $\mathfrak{p}$ it is easy to see the following:

i) $\mathfrak{p}$ is generated by a prime element π. We shall call it the ***uniformizer***.

ii) Every non-zero ideal $\mathfrak{q} \subseteq A$ is generated by a power of the uniformizer, i.e. $\mathfrak{q} = \langle \pi^n \rangle = \mathfrak{p}^n$, for some unique $n \geq 0$.

iii) $A^* = A - \mathfrak{p}$, the units are the complement of $\mathfrak{p}$ in A.

iv) All the irreducible elements of A are of the form $\pi\epsilon$, where $\epsilon \in A^*$.

v) $\forall x \in A$, $x = \pi^m \epsilon$, $m \geq 0$ and $\epsilon \in A^*$. x is not a unit if and only if $m > 0$.

With this in mind, we can define a map $v \colon A \to \mathbb{N}$, putting $v(\pi^m \epsilon) = m$. If K is the field of fractions of A, we can extend the map to K^* in a natural way, observing that for every $x \in K^*$ we have

$$x = \frac{\pi^n \epsilon}{\pi^m \gamma} = \pi^{n-m} \alpha,$$

where ϵ, γ and α are in A^*. Therefore, we can extenddefine $v : K^* \to \mathbb{Z}$ setting $v(x) = v(\pi^n \alpha) = n \in \mathbb{Z}$ for every $x \neq 0$.

This mapping satisfies the following properties:

i) It is a group morphism, i.e. $v(xy) = v(x) + v(y)$ $\forall x, y \in K^*$.

ii) $v(x + y) \geq \min(v(x), v(y))$.

Definition 1.3. *Let K be a field. A **discrete valuation** on K is a group morphism $v : K^* \to \mathbb{Z}$ satisfying property ii).*

The image of v in $\mathbb{Z}$ will be a subgroup of $\mathbb{Z}$, and so will either be equal to $\{0\}$ or to $n\mathbb{Z}$, for some $n \geq 1$. We will distinguish between trivial and non-trivial valuations, since the first ones aren't very interesting.

With this in mind, let K be a field with a non-trivial discrete valuation $v : K^* \to \mathbb{Z}$. We can define the ring

$$A = \{x \in K^* | v(x) \geq 0\} \cup \{0\}$$

and the ideal

$$\mathfrak{p} = \{x \in K^* | v(x) > 0\} \cup \{0\}.$$

This definition makes A a discrete valuation ring with non-zero prime ideal $\mathfrak{p}$, and with field of fractions K. Any element $\pi \in A$ with $v(\pi) = n$ will be a generator of $\mathfrak{p}$. If we rescale the function v such that $v(\pi) = 1$, we will call this element a uniformizer.

Definition 1.4. *For a field K, an **absolute value** is a function $|\cdot| : K \to \mathbb{R}$ such that*

i) $|x| > 0$ *for* $x \in K^*$ *and* $|0| = 0$.

ii) $|xy| = |x||y|$.

iii) $|x + y| \leq |x| + |y|$.

*We say it is **non-archimedean** if we also have* $|x + y| \leq \max\{|x|, |y|\}$.

Again, we distinguish between trivial and non-trivial absolute values, restricting ourselves to the second kind.

On the other hand, if we have a discrete valuation ring A with field of fractions K, we can endow K with an absolute value. Let $c \in \mathbb{R}$ such that $0 < c < 1$. We define

$$|\alpha| = c^{v(\alpha)} \ \forall \alpha \in K^*,$$

and $|0| = 0$. It can be easily checked that this is indeed an absolute value, and in particular, a non-archimedean one.

Let K be a field with non-archimedean absolute value $|\cdot|$, and let $a_1, \ldots, a_n \in K$. Then we have:

$$i) \ \Big| \sum_{1 \leq i \leq n} a_i \Big| \leq \max_{1 \leq i \leq n} \{|a_i|\}. \tag{1}$$

$$ii) \ a_1 + \cdots + a_n = 0 \implies \text{at least two } a_i, a_j \text{ have maximum absolute value.} \tag{2}$$

The first statement is true by induction. For the second one, suppose that a_j were such that $|a_j| > |a_k|$ for all $k \neq j$. Since we have that $|a_j| = |\sum_{i \neq j} a_i| \leq \max_{i \neq j}\{|a_i|\}$, we'd arrive at a contradiction.

Now let K be a field with an absolute value, not necessarily non-archimedean. We can consider K to be a one dimensional K-vector space, and so $|\cdot|$ is a norm over K. This norm induces a metric, and hence also a topology, on K. Therefore we can consider the notion of completeness, that is, whether every Cauchy sequence converges to a limit in K.

Theorem 1.5. *For every field K with an absolute value, there exists a unique complete valued field $\widehat{K}$ with $K \subseteq \widehat{K}$ preseving the absolute value on K and such that K is dense in $\widehat{K}$.*

We call such a field $\widehat{K}$ the ***completion of*** K with respect to the valuation $|\cdot|$. We can construct this field explicitly taking the set of equivalence classes of Cauchy sequences of K, where we consider two sequences to be equivalent when the limit of their difference is 0. This is a common construction in analysis.

Example: i) Let $|\cdot|$ be the usual absolute value on $\mathbb{R}$ restricted to $\mathbb{Q}$. Then the completion of $\mathbb{Q}$ is precisely $\mathbb{R}$.

ii) The p-adic numbers $\mathbb{Q}_p$, which we shall define and study in more detail in the next chapter, are the completion of $\mathbb{Q}$ with respect to the p-adic absolute value.

Definition 1.6. *A **local field** K is a field with a non-trivial absolute value such that K is locally compact.*

We will see in chapter 3 that every finite extension of $\mathbb{Q}_p$ is a local field. In contrast, we say K is a ***global field*** if it is a finite extensions of either $\mathbb{Q}$ or $\mathbb{F}_q(t)$, where $\mathbb{F}_q$ is the finite field with q elements. We will only be studying fields with characteristic 0, so whenever we say K is a global field, we will be referring to a number field.

Proposition 1.7. *Let K be a field with a discrete valuation v and discrete valuation ring A and uniformizer π. Then K is a local field if and only if K is complete and the residue field $A/\pi A$ is finite.*

In chapter 3 we study extensions of local fields, and we are interested in extending the absolute value defined on the base field to its extension. For this, we use field norms. Let K a field and L a finite extension of K. Then L is a finite dimensional vector space over K, and for each $\alpha \in L$, the function $m_\alpha(x) = \alpha x$ is K-linear. If $\alpha \neq 0$, its determinant is different from 0.

Definition 1.8. *For every $\alpha \in L$, $\alpha \neq 0$, we define the **norm of** α **over** K as $\mathrm{N}_{L/K}(\alpha) = \det(m_\alpha) \in K^*$.*

The mapping $\mathrm{N}_{L/K} : L^* \to K^*$ is a group homomorphism, and so for every $\alpha, \beta \in L$, we have $\mathrm{N}_{L/K}(\alpha\beta) = \mathrm{N}_{L/K}(\alpha)\,\mathrm{N}_{L/K}(\beta)$. For every $a \in K$, $\mathrm{N}_{L/K}(a) = a^{[L:K]}$. We can extended $\mathrm{N}_{L/K}$ to L, setting $\mathrm{N}_{L/K}(0) = 0$. The norm function behaves well for towers of finite field extensions $M/L/K$:

$$\mathrm{N}_{M/K}(x) = \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L}(x), \ \forall x \in M$$

There are several equivalent ways to calculate the norm of an element. We list them here:

1. Let $f(X)$ be the minimal polynomial of $\alpha \in L$ over K. Set $n = [K(\alpha) : K]$, and let a_0 be the constant term of $f(X)$. Then $\mathrm{N}_{L/K}(\alpha) = ((-1)^n a_0)^{[L:K(\alpha)]}$.

2. Let $\alpha_1, \ldots, \alpha_n$ be the roots of the minimal polynomial of $\alpha \in L$ over K in some splitting field, and let $m = [L : K(\alpha)]$. We can calculate the norm of α as : $\mathrm{N}_{L/K}(\alpha) = (\prod_{i=1}^{n} \alpha_i)^m$.

3. If L is Galois over K, set $G = \mathrm{Gal}(L/K)$. In this case we have that $\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in G} {}^{\sigma}\alpha$.

The reader can find the details for these equivalent definitions in chapter 5 of [Mil17b].

1.2 Dedekind Domains

Another important concept of algebraic number theory that is key for our proof of the Kronecker-Weber theorem is that of Dedekind domain. This mathematical object is at the heart of ramification theory, and it is of special interest for being a ring with a unique factorization of ideals. Most of the results of this subsection can be found in chapter 3 of [Mil17a].

Definition 1.9. *Let A be an integral domain that is not a field. We say that A is a* ***Dedekind Domain*** *if every non-zero proper ideal factors uniquely into the product of prime ideals. In other words, if for every proper non-zero ideal $\mathfrak{I} \in A$ there exist unique distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s \in A$ and $r_1, \ldots, r_s > 0$ such that*

$$\mathfrak{I} = \mathfrak{p}_1^{r_1} \ldots \mathfrak{p}_s^{r_s}.$$

These prime ideals, together with their exponents, are uniquely defined by the ideal $\mathfrak{I}$.

Example: for a finite extension K of $\mathbb{Q}$ we define its ring of integers as the set of roots of monic polynomials with integer coefficients, which we denote by $\mathcal{O}_K$. It is the classical example of Dedekind Domain, and you can find a proof of it in chapters 5 and 6 of [Ste04].

Proposition 1.10. *An integral domain A is a Dedekind Domain if and only if it is Noetherian(i.e. every ideal is finitely generated), integrally closed and every non-zero prime ideal is maximal.*

This is the usual (and technical) definition of a Dedekind Domain, whereas the definition we've chosen is usually the first basic result. As our objective goes far beyond studying Dedekind Domains, taking the conceptual definition as our starting point is good enough. For a detailed introduction to Dedekind Domains, refer to chapter 3 from [Mil17a].

Proposition 1.11 (Proposition 3.2 in [Mil17a])**.** *A local integral domain is a Dedekind Domain if and only if it is a discrete valuation ring.*

Proposition 1.12 (Propostion 3.4 in [Mil17a])**.** *A Noetherian integral domain A is a Dedekind Domain if and only if, for every non-zero prime ideal $\mathfrak{p}$, the localization $A_{\mathfrak{p}}$ is a discrete valuation ring.*

Unless otherwise noted, from here on let A be a Dedekind domain, K its field of fractions and let L be finite separable field extension of K with $n = [L : K]$. Let $B = \overline{A}$, the integral closure of A in L. By Proposition 3.29 in [Mil17a], B will also be Dedekind Domain, and so each prime ideal $\mathfrak{p}$ of A factors in B:

$$\mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}$$

This is the main interest in ramification theory: to study how a prime ideal $\mathfrak{p}$ in A ramifies in the finite extensions B of A.

For each $\mathfrak{q}$ in the factorization of $\mathfrak{p}$, we say $\mathfrak{q}$ divides $\mathfrak{p}$ and write $\mathfrak{q} \mid \mathfrak{p}$. We write $e_{\mathfrak{q}/\mathfrak{p}}$ or $e_{\mathfrak{q}/\mathfrak{p}}(L/K)$ for the exponent of $\mathfrak{q}$ in the factorization of $\mathfrak{p}$, which we shall call the ***ramification index***. Since $\mathfrak{p}$ and $\mathfrak{q}$ are both prime ideals in their respective rings, the quotients $A/\mathfrak{p} \subseteq B/\mathfrak{q}$ will be fields, and we define the ***residue class degree*** as $f_{\mathfrak{q}/\mathfrak{p}}(L/K) = f_{\mathfrak{q}/\mathfrak{p}} = [B/\mathfrak{q} : A/\mathfrak{p}]$.

Proposition 1.13. *For every prime ideal $\mathfrak{p}$ of A, let e_i, f_i be the ramification indices and residue class degree of $\mathfrak{p}$ in L. Then we have*

$$\sum_{i=1}^{g} e_i f_i = n = [L : K].$$

Moreover, if L is Galois over K, $\mathrm{Gal}(L/K)$ acts transitively over the primes $\mathfrak{q}$ lying over $\mathfrak{p}$. In particular, all the e_i are equal, as well as the f_i and we have

$$efg = n.$$

If any of the ramification indices for a prime $\mathfrak{p}$ is greater than 1, we say that $\mathfrak{p}$ ***ramifies*** in B (or in L). We say $\mathfrak{p}$ is ***totally ramified*** at $\mathfrak{q}$ if $e_{\mathfrak{q}/\mathfrak{p}} = [L : K]$, equivalently if $f_{\mathfrak{q}/\mathfrak{p}} = g_{\mathfrak{p}} = 1$. We say that $\mathfrak{p}$ is ***unramified*** at $\mathfrak{q}$ if $e_{\mathfrak{q}/\mathfrak{p}} = 1$. A prime $\mathfrak{p}$ is said to ***split*** or split completely in L if $e_i = f_i = 1$ for all i, and is said to be ***inert*** if $\mathfrak{p}B$ is a prime ideal in B, i.e $e = g = 1$.

Let $C/B/A$ be finite extensions of Dedekind domains, with respective field of fractions $M/L/K$, and let $\mathfrak{P}, \mathfrak{q}$ and $\mathfrak{p}$ prime ideals of M, L and K respectively, with $\mathfrak{P} \mid \mathfrak{q} \mid \mathfrak{p}$. Then the ramification index and the residue degree are multiplicative:

$$e_{\mathfrak{P}/\mathfrak{p}} = e_{\mathfrak{P}/\mathfrak{q}} \cdot e_{\mathfrak{q}/\mathfrak{p}}$$
$$f_{\mathfrak{P}/\mathfrak{p}} = f_{\mathfrak{P}/\mathfrak{q}} \cdot f_{\mathfrak{q}/\mathfrak{p}}$$

A useful invariant for determining which primes ramify in a given extension is the ***discriminant***. Let $A \subseteq B$ be Dedekind domains, and assume B is a free rank A-module, of rank $m < \infty$. Let $\beta_1, \ldots, \beta_m$ be a basis of B, the discriminant of B over A is

$$\mathrm{disc}(B/A) = (\det(\mathrm{Tr}_{B/A}(\beta_i \beta_j))),$$

that is, the ideal generated by $\det(\mathrm{Tr}_{B/A}(\beta_i \beta_j))$, where $\mathrm{Tr}_{B/A}$ is the trace map.

Theorem 1.14. *Under the assumptions of this section(i.e. A Dedekind domain, L finite extension of its field of fractions,...), if B is a free rank A-module, a prime* $\mathfrak{p}$ *ramifies in L if and only if* $\mathfrak{p} | \ disc(B/A)$. *In particular, only a finite number of prime ideals ramify.*

You can find a detailed proof in [Mil17a], it is numbered as theorem 3.35.

Another important invariant for studying the ramification is the discriminant of a polynomial:

Definition 1.15. *Let K be a field with characteristic 0, and let* $f \in K[X]$ *be a monic polynomial of degree* $n \geq 1$. *Let* $f(X) = \prod_i (X - \alpha_i)$ *in some splitting field over K. The* ***discriminant of*** *f is:*

$$D(f) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(\alpha_i).$$

Proposition 1.16. *Let K be the fraction field of a Dedekind domain A. Let* $L = K(\alpha)$ *be a finite extension of K, B the integral closure of A in L and let f be the irreducible polynomial of* α. *Then, we have that*

$$\text{disc}(B/A) \mid (D(f)).$$

See [Mil17a] Proposition 2.34 and Proposition 2.24. As a corollary, we get that if a prime $\mathfrak{p}$ doesn't divide $(D(f))$, it will be unramified in L.

1.3 Finitely Generated Groups

A very useful result in group theory is the structure theorem of finitely generated Abelian groups. It will also help us to simplify the Kronecker-Weber theorem's proof, since it enables us to consider only extensions with cyclic Galois group. We state it as follows:

Theorem 1.17. *Let G be a finitely generated abelian group. Then* $\exists\ n_1, \ldots, n_s, r \in \mathbb{N}$ *with* $n_1 > 1, r \geq 0$ *and* $n_1 \mid n_2 \mid \cdots \mid n_s$ *such that:*

$$G \cong (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_s\mathbb{Z}) \times \mathbb{Z}^r$$

Moreover, the n_i *and r determine the isomorphism class of G.*

In particular, if G is a finite abelian group, then G is isomorphic to the product of finitely many finite cyclic groups.
You can find a simple exposition of the proof of the theorem in chapter 3 of [Ste04].

A useful result in the study of cyclotomic extensions is the description of the multiplicative groups of $\mathbb{Z}/nZ$.

Proposition 1.18. *Let p be a prime. Then we have:*
If $p \neq 2$, $(\mathbb{Z}/p^n\mathbb{Z})^*$ *is cyclic for every* $n \geq 1$.
If $p = 2$, $(\mathbb{Z}/2^n\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$, *for* $n \geq 3$.
$(\mathbb{Z}/2^2\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$ *and* $(\mathbb{Z}/2\mathbb{Z})^* \cong \{1\}$ *complete the list.*

1.4 Motivational example

Let's show the principal motivation for the Kronecker-Weber theorem. Namely, that every abelian finite group is Galois over $\mathbb{Q}$ as a subfield of a cyclotomic extension of $\mathbb{Q}$. First we will study Galois groups of cyclotomic extension. Let K be a field and let $m \geq 1$ be prime to the characteristic of K. Then, $X^m - 1$ is separable in $K[X]$. This means that there will be exactly m different m-th roots of unity in some splitting field over K. Let ζ_m be primitive m-root of unity, i.e. a generator of the group of m-th roots of unity, and let $f(x)$ be the its irreducible polynomial in $K[X]$. Consider $L = K(\zeta_m)$. Since ζ_m generates all the m-th roots of unity, L will be the splitting field of $X^m - 1$ over K, and as a result L will be Galois over K

Theorem 1.19. *For every $m \geq 1$ prime to the characteristic of K, we have that the Galois group $G = \mathrm{Gal}(K(\zeta_m)/K)$ is isomorphic to a subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$.*

Proof. Let $\sigma \in G$, then σ permutes the roots of $f(x)$, and so $\sigma(\zeta_m) = \zeta_m^{i(\sigma)}$ for some $i(\sigma) \in \mathbb{Z}/m\mathbb{Z}$. As ζ_m is a primitive root of unit, $\sigma(\zeta_m)$ must also be a primitive root of unity. Therefore $(i(\sigma), m) = 1$ and $i(\sigma) \in (\mathbb{Z}/m\mathbb{Z})^*$. This way we can define a mapping i:

$$i : G \to (\mathbb{Z}/m\mathbb{Z})^*$$

We want to show that i is a group morphism and also injective. Let $\tau, \sigma \in G$, we calculate:

$$\tau\sigma(\zeta_m) = \zeta_m^{i(\tau\sigma)} = \tau(\sigma(\zeta_m)) = \tau(\zeta_m^{i(\sigma)}) = (\zeta_m^{i(\sigma)})^{i(\tau)} = \zeta_m^{i(\tau)i(\sigma)}$$

Therefore, $i(\tau\sigma) \equiv i(\tau)i(\sigma) \mod m$, so i is a morphism. Since the image of ζ_m by an element σ of G uniquely characterizes σ, we can conclude that the morphism will be injective.

□

Corollary 1.20. *For every $m \geq 1$, $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$.*

Proof. We know that for $\mathbb{Q}$, the irreducible polynomial for ζ_m is the m-th cyclotomic polynomial, which is irreducible and of degree $\varphi(m)$. Hence, $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m) = |(\mathbb{Z}/n\mathbb{Z})^*|$ and the morphism i defined in the previous proof is a isomorphism. □

Proposition 1.21. *$\forall\ n > 1$ there exist infinite primes p such that $p \equiv 1 \pmod{n}$.*

Corollary 1.22. *Every finite abelian group A is isomorphic to a subgroup and a quotient of $(\mathbb{Z}/n\mathbb{Z})^*$, for infinite mutually prime integers n.*

Proof. By the structure theorem of finite abelian groups, $A \cong (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_s\mathbb{Z})$, for some $n_i > 1$. By the above proposition, we know that there exist distinct primes $p_1, \ldots, p_s$ such that $p_i \equiv 1 \mod n_i$. As $(\mathbb{Z}/p_i\mathbb{Z})^*$ are cyclic groups of order $p_i - 1$ and $n_i \mid p_i - 1$, they will have both a subgroup and a quotient isomorphic to $(\mathbb{Z}/n_i\mathbb{Z})$. We consider $n = p_1 \cdot \cdots \cdot p_s$, and by the Chinese Remainder Theorem,

$(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/p_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_s\mathbb{Z})^*$, so A will be isomorphic to both a subgroup and a quotient of $(\mathbb{Z}/n\mathbb{Z})^*$. Since we have an infinite number of primes p_i to choose from, we can construct infinitely many integers n satisfying the theorem. Moreover, we can construct these integers so they are all mutually prime. □

Theorem 1.23. *For every finite abelian group G there exist infinitely many finite Galois extensions $L/\mathbb{Q}$ such that* $\mathrm{Gal}(L/\mathbb{Q}) \cong G$.

Proof. Take n so G is isomorphic to a quotient of $(\mathbb{Z}/n\mathbb{Z})^*$ by some subgroup H. Now take $E = \mathbb{Q}(\zeta_n)^H$, which will be Galois over $\mathbb{Q}$ by virtue of H being normal to $(\mathbb{Z}/n\mathbb{Z})^*$ (it is an abelian group) and it's Galois group will be isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*/H \cong G$, as we wanted. Again, we have infinitely many mutually prime integers n satisfying this, so we can construct infinitely many extensions L with Galois group isomorphic to A. □

As I mentioned in the introduction, the Kronecker-Weber theorem doesn't hold for number fields in general. We won't prove this here, but we illustrate it with an example.

Consider $K = \mathbb{Q}(\sqrt{2})$ and let $L = \mathbb{Q}(\sqrt[4]{2})$. We have that L/K is Galois and $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$, so it is an abelian extension. However, L isn't contained in any cyclotomic extension of K.

Since $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$, any cyclotomic extension F of K will be contained in a cyclotomic extension of $\mathbb{Q}$, taking the compositum $F \cdot \mathbb{Q}(\zeta_8)$. Hence, if L were contained in a cyclotomic extension of K, it would also be a subfield of an abelian extension of $\mathbb{Q}$, and so it would be Galois over $\mathbb{Q}$. However, the irreducible polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$, $X^4 - 2$, also has $i\sqrt[4]{2}$ as a root. This root doesn't live in L, so L isn't Galois over $\mathbb{Q}$, and we arrive at a contradiction.

2 The Field of p-adic Numbers

There are basically two ways to define the p-adic numbers: an "analytical" definition as the completion of $\mathbb{Q}$ with respect to a certain norm (the p-adic absolute value) and an "algebraic" definition as a projective limit of rings. In this chapter we discuss both definitions, and see their equivalence. We finish the chapter with the first important result for $\mathbb{Q}_p$, Hensel's lemma, a way to see if certain polynomials have roots in $\mathbb{Q}_p$, and with a brief overview of analysis in $\mathbb{Q}_p$.

2.1 Algebraic Definition

This section is rather technical, but the results shown in it are the basis for the rest of the text. We follow professor Jordi Quer's lecture notes on the p-adic numbers found in [Que11]. Let p be a prime integer. To construct the field of p-adic numbers we need to use some algebraic concepts, namely projective limits:

Definition 2.1. *Let I be a set with a partial order $\leq$. A **projective system of rings** is a family of rings $\{G_i\}_{i\in I}$ and ring morphisms $f_{ij} : G_i \to G_j$, whenever $i \geq j$, such that $f_{jk} \circ f_{ij} = f_{ik}$ for all $i \geq j \geq k$ and $f_{ii} = Id_{G_i}$.*
*We define it's **projective limit** to be*

$$G = \varprojlim_{i\in I} G_i = \{(g_i)_{i\in I} \in \prod_{i\in I} G_i \mid g_j = f_{ij}(g_i) \ \forall \ i \geq j\}.$$

The concept of projective limit can be defined for any other category, but we will only consider the case of rings.

We can take the rings $G_n = \mathbb{Z}/p^n\mathbb{Z}$ for $n \geq 1$ and $f_{mn} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ with $f([a]_{p^m}) = [a]_{p^n}$, with $m \geq n$. The mappings f_{mn} are ring morphisms satisfying the projective system hypothesis. Therefore we can consider it's projective limit.

Definition 2.2. *We define the p-adic integers, which we denote by $\mathbb{Z}_p$, as*

$$\mathbb{Z}_p = \varprojlim_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z} = \{(a_n)_{n\geq 1} \mid a_n \in \mathbb{Z}/p^n\mathbb{Z}, \ a_m \equiv a_n \pmod{p^n} \ \forall \ n \geq m\}.$$

We define the operations sum and multiplication in the natural way :

$$(a_n)_{n\geq 1} + (b_n)_{n\geq 1} = (a_n + b_n)_{n\geq 1}, \ (a_n)_{n\geq 1}(b_n)_{n\geq 1} = (a_n b_n)_{n\geq 1}.$$

They are well defined, since reducing an integer modulo p^n is commutative with the operations sum and multiplication. We can take $(1)_{n\geq 1}$ and $(0)_{n\geq 1}$ as the multiplicative and additive identities. With this we see that $\mathbb{Z}_p$ is a commutative ring. We can embed the integers $\mathbb{Z}$ in $\mathbb{Z}_p$: for every $a \in \mathbb{Z}$ we can consider $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ such that $a_n \equiv a \pmod{p^n}$. Then, we identify a with $(a_n)_{n\geq 1}$ in $\mathbb{Z}_p$.

Proposition 2.3. *The ring of p-adic integers is an integral domain.*

Proof. Let $\alpha = (a_n)_{n\geq 1}, \beta = (b_n)_{n\geq 1} \in \mathbb{Z}_p$, with $\beta \neq 0$ and $\alpha\beta = 0$. It is clear by the definition of $\mathbb{Z}_p$ that if an element $(b_n)_{n\geq 1} \in \mathbb{Z}_p$ has n-th component equal to 0, then all its m-th components will also be 0, for $m \leq n$. With this in mind, since $\beta \neq 0$, we can set m to be the largest integer such that b_m is 0. We have that m is a positive integer and that $b_{m+1} \neq 0$.

We know that for every $n \geq m+1$, $b_n \equiv b_{m+1} \neq 0 \pmod{p^{m+1}}$ which means that $p^{m+1} \nmid b_n$. However, as $b_n \equiv b_m = 0 \pmod{p^m}$, we can write $b_n = p^m c_n$, with c_n not divisible by p.

Now consider $n \geq 1$. As $0 = a_{n+m}b_{n+m} = a_{n+m}p^m c_{n+m} \pmod{p^{m+n}}$, we have that $a_{n+m}c_{n+m} = 0 \pmod{p^n}$ and so $a_{n+m} = 0 \pmod{p^n}$. This implies that $a_n = 0$, for every $n \geq 1$, just as we wanted to see. □

For $r \geq 1$, let's denote by red_r the morphism from $\mathbb{Z}_p$ to $\mathbb{Z}/p^r\mathbb{Z}$ that sends every p-adic integer to its r-th component: $\mathrm{red}_r((a_n)_{n\geq 1}) = a_r$. This notation is very useful to write down results in a compact way.

Proposition 2.4. *For every $r \geq 1$, we have an exact sequence:*

$$0 \to \mathbb{Z}_p \xrightarrow{p^r} \mathbb{Z}_p \xrightarrow{red_r} \mathbb{Z}/p^r\mathbb{Z} \to 0$$

where p^r denotes multiplying precisely by p^r. We deduce that $\mathbb{Z}_p/p^r\mathbb{Z}_p \cong \mathbb{Z}/p^r\mathbb{Z}$.

Proof. To see the multiplying by p^r is one-to-one, we have enough with proving it for $r = 1$: then all we need to do is compose n times and we get that multiplying by p^r is also one-to-one. Suppose $\alpha = (a_n)_{n\geq 1}$ is such that $p\alpha = (pa_n)_{n\geq 1} = 0$. Then we have $pa_{n+1} \equiv 0 \pmod{p^{n+1}}$ for every $n \geq 1$, and so $a_{n+1} \equiv 0 \pmod{p^n}$. Since $a_n \equiv a_{n+1} \pmod{p^n}$, we have that $a_n = 0,\ \forall n \geq 1$, so $\alpha = 0$.

For the next part, we need to see that $p^r\mathbb{Z}_p = \ker(\mathrm{red}_r)$. One inclusion is obvious, since $\forall \alpha \in p^r\mathbb{Z}_p$ we have that $\mathrm{red}_r(\alpha) = p^r b_r = 0 \pmod{p^r}$. Now suppose $\alpha = (a_n)_{n\geq 1}$ is such that $\mathrm{red}_r(\alpha) = 0$. This tells us that $\forall k \geq 1$, $a_{r+k} \equiv a_r = 0 \pmod{p^r}$, so a_{r+k} is divisible by p^r. For every $k \geq 1$, take b_k to be such that $a_{r+k} = p^r b_k$. Then we have that $p^r b_{k+1} \equiv p^r b_k \pmod{p^{r+k}}$, which means that $b_{k+1} \equiv b_k \pmod{p^k}$, and so $\beta = (b_k)_{k\geq 1}$ defines a p-adic number. Therefore, $\alpha = p^r\beta \in p^r\mathbb{Z}_p$, as we wanted to see.

It's clear to see that red_n is onto: we just need to consider integers with the corresponding residue class in $\mathbb{Z}/p^n\mathbb{Z}$. □

Now we are ready to prove the next important proposition:

Proposition 2.5. *The p-adic integers are a unique factorization domain (UFD) with a unique prime up to associates: p. In other words, every $\alpha \in \mathbb{Z}_p$ can be written uniquely as:*

$$\alpha = p^r\epsilon, \quad r \geq 0, \quad \epsilon \in \mathbb{Z}_p^*.$$

Proof. Let's begin by observing that $\alpha = (a_n)_{n\geq 1} \in \mathbb{Z}_p^*$ if and only if $a_1 \neq 0$. We know $a_1 \neq 0 \pmod{p}$ if and only if p and a_1 are coprime. Therefore, for every $n \geq 1$,

$a_n \equiv a_1 \neq 0 \pmod{p}$, so p^n will also be coprime to a_n. Thus, we will have an inverse of a_n in $\mathbb{Z}/p^n\mathbb{Z}$ for every $n \geq 1$, let's denote it by b_n. These inverses form a sequence $(b_n)_{n\geq 1}$ that will be the inverse of α in $\mathbb{Z}_p$. Reciprocally, if $a_1 = 0$, then for every $\beta \in \mathbb{Z}_p$ we'll have that $\mathrm{red}_1(\alpha\beta) = 0$, so $\alpha\beta \neq 1$. Thanks to our the previous observation, we can assure that $\mathbb{Z}_p^* = \mathbb{Z}_p - p\mathbb{Z}_p$.

Now, if $\alpha = (a_n) \in \mathbb{Z}_p^*$ is not zero, take $r \geq 0$ to be the biggest integer such that $a_r = 0$. Again by the previous observation, we have that $\alpha \in p^r\mathbb{Z}_p$ but $\alpha \notin p^{r+1}\mathbb{Z}_p$, so $\alpha = p^r\epsilon$, with $\epsilon \in \mathbb{Z}_p - p\mathbb{Z}_p = \mathbb{Z}_p^*$.

To finish off, suppose $\alpha = p^r\epsilon = p^s\gamma$, with $r \geq s$. We get $p^s(p^{r-s}\epsilon - \gamma) = 0$. As we have seen that the p-adic integers are an integral domain and $p^s \neq 0$, we must have $p^{r-s}\epsilon = \gamma$. But as $\gamma \in \mathbb{Z}_p^*$, $\mathrm{red}_1(p^{r-s}\epsilon) \neq 0$ and necessarily $r = s$, so $\epsilon = \gamma$. □

Let $\mathfrak{p} \subseteq \mathbb{Z}_p$ be an ideal. Let $x = p^t u \in \mathfrak{p},\ u \in \mathbb{Z}_p^*$ be such that for every $y = p^s v \in \mathfrak{p}$ with $v \in Z_p^*$, $0 \leq t \leq s$. Then it's easy to see that $\mathfrak{p} = p^t\mathbb{Z}_p$, and so $\mathbb{Z}_p$ is an DIP with only one maximal ideal: $p\mathbb{Z}_p$. Therefore, $\mathbb{Z}_p$ is a discrete valuation ring, and its non-zero ideals are of the form $p^n\mathbb{Z}_p$ for some $n \geq 0$.

Definition 2.6. *As $\mathbb{Z}_p$ is an integral domain, we can consider its field of quotients, which we shall denote by $\mathbb{Q}_p$, the **field of p-adic numbers**.*

Observe that, as $\mathbb{Z}$ is in $\mathbb{Z}_p$, $\mathbb{Q}$ will be a subfield of $\mathbb{Q}_p$, and so its characteristic will be equal to 0.

Now we are in conditions to define the p-adic valuation and the p-adic absolute value, which will be very useful tools. We define them just as we would for any other DVR, but to highlight their importance, we give them a proper name.

Definition 2.7. *The **p-adic valuation** v_p is the natural valuation defined on $\mathbb{Q}_p$: That is, for every $\alpha = p^r\epsilon \in \mathbb{Q}_p^*$,*

$$v_p(\alpha) = r \in \mathbb{Z}$$

*The **p-adic absolute value** $|\cdot|_p$ or $|\cdot|$ is defined as $|0| = 0$ and, for $\alpha \in \mathbb{Q}_p^*$,*

$$|\alpha| = p^{-v_p(\alpha)}.$$

Some texts also put $v_p(0) = \infty$, but this is just a convention, and we won't actually need this.

We have a topology on $\mathbb{Q}_p$ induced by the p-adic distance:

$$d(\alpha, \beta) = |\alpha - \beta| = p^{-v(\alpha-\beta)}.$$

Let's consider $\alpha \in \mathbb{Q}_p, \epsilon > 0$ and let's denote by $B(\alpha, \epsilon)$ the open ball of radius ϵ and center α:

$$|\beta - \alpha| = p^{-v_p(\beta-\alpha)} < \epsilon \iff v_p(\beta - \alpha) > -\log_p(\epsilon) \iff v_p(\beta - \alpha) \geq \lfloor 1 - \log_p(\epsilon) \rfloor.$$

This happens if and only if $\beta \in \alpha + p^r\mathbb{Z}_p,\ r = \lfloor 1 - \log_p(\epsilon) \rfloor$. Therefore we can write:

$$B(\alpha, \epsilon) = \alpha + p^r\mathbb{Z}_p,\ r = \lfloor 1 - \log_p(\epsilon) \rfloor.$$

With this we see that the topology we have defined on $\mathbb{Q}_p$ is generated by the open sets $\alpha + p^r\mathbb{Z}_p,\ \alpha \in \mathbb{Q}_p,\ r \geq 0$.

Theorem 2.8. *The topological field $\mathbb{Q}_p$ is complete.*

Proof. We start by seeing that $\mathbb{Z}_p$ is complete. Let's observe that a Cauchy sequence $(\alpha_n)_{n\geq 1}$ in $\mathbb{Z}_p$ will satisfy that for every $k \geq 0$ there exists a n_k such that for $n, m \geq n_k$, $d(\alpha_n, \alpha_m) \leq p^{-k}$. That is, $v_p(\alpha_n - \alpha_m) \geq k$. We can also take the n_k to be increasing: $n_{k+1} \geq n_k$. Let a_k be an integer such that $a_k \equiv \alpha_{n_k} \pmod{p^k}$. Then we have that $a_{k+1} \equiv \alpha_{n_{k+1}} \equiv \alpha_{n_k} \equiv a_k \pmod{p^k}$. The p-adic integer defined by $(a_k)_{k\geq 1} = \alpha$ will be the limit of our sequence v_p, as $v_p(\alpha_n - \alpha) \geq k$, if $n \geq n_k$.

Now let $(\alpha_n)_{n\geq 1}$ be a Cauchy sequence in $\mathbb{Q}_p$. Our aim is to see that for some $r \geq 0$, $\alpha_n \in p^{-r}\mathbb{Z}_p\ \forall n \geq 0$, . Then multiplying every element by p^r we have a Cauchy sequence in $\mathbb{Z}_p$, which must have a limit $\alpha \in \mathbb{Z}_p$. Then $p^{-r}\alpha \in \mathbb{Q}_p$ will be the limit to our original Cauchy sequence.

We saw earlier that we can take a n_0 such that for every $n \geq n_0$ we have that $v_p(\alpha_n - \alpha_{n_0}) \geq 0$. This means that $\alpha_n \in \alpha_{n_0} + \mathbb{Z}_p,\ \forall n \geq n_0$. Now take r an integer big enough so $p^r\alpha_n \in \mathbb{Z}_p$ for every $n \leq n_0$. Then we'll also have $p^r\alpha_n \in p^r\alpha_{n_0} + p^r\mathbb{Z}_p \subseteq \mathbb{Z}_p$ for $n \geq n_0$, as we wanted to see.

□

Proposition 2.9. *$\mathbb{Z}_p$ is a compact set in $\mathbb{Q}_p$, and $\mathbb{Q}_p$ is locally compact.*

Proof. As $\mathbb{Z}_p$ is a neighbourhood of 0, if we see that $\mathbb{Z}_p$ is compact, we'll see that every element $\alpha \in \mathbb{Q}_p$ has a compact neighbour, namely $\alpha + \mathbb{Z}_p$.

It is a standard result in analysis that a subset of a metric space is compact if and only if it is complete and totally bounded (i.e. for every $\epsilon > 0$, there is a finite number of open balls of radius ϵ that cover the subset).

We have just seen that $\mathbb{Z}_p$ is complete, so we only need to show that it is also totally bounded. It's enough to consider ϵ to be a negative power of p, as these are the only possible values of $|\cdot|_p$ over $\mathbb{Z}_p$. Fix p^{-n}, with $n \geq 0$. We know that $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$, so let's take $a_1, \ldots, a_{p^n} \in \mathbb{Z}_p$, representatives of the cosets of $\mathbb{Z}_p/p^n\mathbb{Z}_p$. Now we have that

$$\mathbb{Z}_p = \bigcup_{i=1}^{p^n}(a_i + p^n\mathbb{Z}_p) = \bigcup_{i=1}^{p^n}(B(a_i, p^{-n}),$$

just as we wanted to see. □

Proposition 2.10. *$\mathbb{Z}$ is dense in $\mathbb{Z}_p$, and so is $\mathbb{Q}$ in $\mathbb{Q}_p$.*

Proof. Any element $\alpha = (a_n)_{n\geq 1} \in \mathbb{Z}_p$ can be seen as the limit of the $a_n \in \mathbb{Z}$. Indeed, $v_p(\alpha - a_n) \geq n$, which tends to infinity, and so the distances will tend to 0. In a very similar way, any p-adic number $\alpha = p^r\epsilon$, with $\epsilon = (a_n) \in \mathbb{Z}_p^*$ and $r \in \mathbb{Z}$, is the limit of the sequence $p^{-r}a_n \in \mathbb{Q}$. □

2.2 Analytical Definition

Again, let p be a prime number. In the previous chapter we saw that $\mathbb{Q}_p$ was a complete normed space, with absolute value $|\cdot|_p$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic absolute value restricted to $\mathbb{Q}$.

Now we would like to define an absolute value on $\mathbb{Q}$ such that it is equivalent to the p-adic absolute value restriced to $\mathbb{Q}$, but without having to rely on the construction of the previous section.

For any non-zero integer a, there is unique maximal power of p that divides it. That is, there exists an $n \geq 0$ such that $p^n \mid a$ and $p^{n+1} \nmid a$. We define the valuation of a as this number: $v_p(a) = n$. If we take a non-zero rational number $\alpha = a/b$, we can define its valuation in a similar way: $v_p(\alpha) = v_p(a) - v_p(b)$. This definition does not depend on the choice of a and b.

Now, we define the p-adic absolute value in $\mathbb{Q}$ as $|0| = 0$ and

$$|\alpha| = p^{-v_p(\alpha)},$$

for $\alpha \in \mathbb{Q}^*$. These definition is analogous to the p-adic absolute value in $\mathbb{Q}_p$ that we gave in the previous chapter. Since this absolute value comes from a discrete valuation, it is also non-archimedean.

Now we can define the field of p-adic numbers as the completion of $\mathbb{Q}$ with respect to $|\cdot|$.

2.3 Hensel's Lemma

In this section we will prove and discuss one of the most important algebraic properties of $\mathbb{Q}_p$, Hensel's Lemma. It gives a method of deciding whether a polynomial in $\mathbb{Z}_p$ has a root, starting from an approximate solution. We will use this result to see which roots of unity live in $\mathbb{Q}_p$ and to study the group $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$

Theorem 2.11 (Hensel's Lemma)**.** *Let $f(X) \in \mathbb{Z}_p[X]$ and suppose $x \in \mathbb{Z}_p$ satisfies*

$$f(x) \equiv 0 \pmod{p^n}.$$

If $k = v_p((f'(x)) < n/2$, then there exists a unique root $\alpha \in \mathbb{Z}_p$ of $f(X)$ such that

$$\alpha \equiv x \pmod{p^{n-k}} \text{ and } v_p(f'(\alpha)) = k.$$

Proof. For the existence, we will construct a Cauchy sequence $(x_m)_{m\geq 0}$ satisfying $f(x_m) \equiv 0 \pmod{p^{n+m}}$ and $v_p(f'(x_m)) = k$, for every $m \geq 0$. We will construct this sequence by iteratively improving the approximate solutions x_m.

Let's begin by considering $x_0 = x$. Take $x_1 = x_0 - f(x_0)/f'(x_0)$. Let's write $f(x_0) = p^n y$ for some $y \in \mathbb{Z}_p$ and $f'(x_0) = p^k u$ for some unit $u \in \mathbb{Z}_p^*$. Then,

$$x_1 - x_0 = -f(x_0)/f'(x_0) = -p^{n-k} y u^{-1} \in p^{n-k}\mathbb{Z}_p$$

Taking the first-order Taylor expansion of $f(X)$, we see that:

$$f(x_1) = f(x_0) + (x_1 - x_0)f'(x_0) + (x_1 - x_0)^2 t,$$

for some $t \in \mathbb{Z}_p$. By the definition of x_1, we get:

$$f(x_1) = (x_1 - x_0)^2 t \in p^{2n-2k}\mathbb{Z}_p \subseteq p^{n+1}\mathbb{Z}_p,$$

since $n > 2k$. Therefore, $f(x_1) \equiv 0 \pmod{p^{n+1}}$.

If we consider the first-order Taylor expansion of $f'(X)$, we get that for some $s \in \mathbb{Z}_p$, $f'(x_1) = f'(x_0) + (x_1 - x_0)s$, . Therefore,

$$f'(x_1) = p^k u + p^{n-k} z = p^k(u + p^{n-2k} z),$$

for some $z \in \mathbb{Z}_p$. Again, since $n > 2k$ and $p \nmid u$, we get:

$$u + p^{n-2k} \in u + p\mathbb{Z}_p \subseteq \mathbb{Z}_p^*$$

This proves $v_p(f'(x_1)) = k$.

We can iterate this construction, taking $x_{m+1} = x_m - f(x_m)/f'(x_m)$, since for every $m \geq 1$, we'll have $f(x_m) \equiv 0 \pmod{p^{n+m}}$ and $m + n > 2k$. These subsequent improvements will satisfy $f(x_m) \equiv 0 \pmod{p^{n+m}}$, $v_p(f'(x_m)) = k$ and $x_{m+1} \equiv x_m \pmod{p^{n+m-k}}$. In particular, they form a Cauchy sequence and since $\mathbb{Z}_p$ is complete, we can take $\alpha \in \mathbb{Z}_p$ to be its limit. Therefore, $f(\alpha) \equiv 0 \pmod{p^{n+m}}$ for all $m \geq 1$, and we can conclude that $f(\alpha) = 0$.

Futhermore, there exists $N > 0$ such that for all $m \geq N$, $v_p(\alpha - x_m) > n - k$, and so $\alpha \equiv x_m \pmod{p^{n-k}}$. But recall that all x_m are equivalent modulo p^{n-k}, so we get $\alpha \equiv x_0 \pmod{p^{n-k}}$, as we wanted.

Let's prove that this α will be unique. Suppose we have ξ, a root of $f(X)$ that satisfies the required conditions. In particular, we have $\alpha \equiv \xi \pmod{p^{n-k}}$, and since $n > 2k$, $n - k \geq k + 1$. So we get

$$\alpha \equiv \xi \pmod{p^{k+1}}.$$

Therefore,

$$f(\xi) = f(\alpha) + f'(\alpha)(\xi - \alpha) + (\xi - \alpha)^2 s$$

for some $s \in \mathbb{Z}_p$. Both α and ξ are roots of $f(X)$, so we get:

$$(\xi - \alpha)(f'(\alpha) + s(\xi - \alpha)) = 0.$$

Now, $v_p(s(\xi - \alpha)) \geq k+1$ and $v_p(f'(\alpha)) = k$, so $f'(\alpha) + s(\xi - \alpha) \neq 0$. We can conclude that $\xi = \alpha$, and so α is unique. □

The condition $2v_p(f'(x)) < n \leq v_p(f(x))$ translates to $|f(x)| < |f'(x)|^2$.

For any element $a \in \mathbb{Z}/p\mathbb{Z}$, when we consider any $\alpha \in \mathbb{Z}_p$ satisfying $\alpha \equiv a \pmod{p}$, we say that we ***lift*** a to $\mathbb{Z}_p$. Analogously, if $f(X) \in F_p[X]$, we can lift f to $g(X) \in \mathbb{Z}_p$ if $f(X) = g(X) \pmod{p}$.

There is another version of Hensel's lemma which is also very useful.

Proposition 2.12 (Hensel's Lemma II)**.** *Let $f(X) \in \mathbb{Z}_p[X]$. Let $\tilde{g}_1(X), \tilde{g}_2(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ be coprime polynomials such that*

$$\tilde{f}(X) = \tilde{g}_1(X)\tilde{g}_2(X),$$

where $\tilde{f}(X)$ is the image of $f(X)$ modulo p. Then there exist $g_1(X), g_2(X) \in \mathbb{Z}_p[X]$ such that $g_i(X) \equiv \tilde{g}_i(X) \pmod{p}$ and

$$f(X) = g_1(X)g_2(X)$$

Now let's use Hensel's lemma to see which roots of unity live in $\mathbb{Q}_p$. First of all, any n-th root of unity $\zeta \in \mathbb{Q}_p$ will satisfy $|\zeta|^n = |\zeta^n| = |1| = 1$, so $|\zeta| = 1$ and therefore, $\zeta \in \mathbb{Z}_p^*$. In particular, each root of unity has a well-defined reduction modulo p. We will show that $\mathbb{Z}_p^*$ contains roots of unity above each element in $\mathbb{F}_p^*$.

For a prime $p \neq 2$, consider $f(X) = X^{p-1} - 1$, with derivative $f'(X) = (p-1)X^{p-2}$. For any element $x \in \mathbb{Z}_p^*$, $v_p(f'(x)) = v_p(p-1) + v_p(x^{p-2}) = 0$. Now, we know that $X^{p-1} - 1$ has $p-1$ distinct roots in $\mathbb{F}_p$: all the elements of $\mathbb{F}_p^*$. Therefore, for each $a \in \mathbb{F}_p^*$, we can take any unit $x \in \mathbb{Z}_p$ such that $x \equiv a \pmod{p}$. We will have $f(x) \equiv 0 \pmod{p}$ and $v_p(f'(x)) = 0 < 1/2$, so we can apply Hensel's Lemma. Therefore, we will have $p-1$ distinct roots of $X^{p-1} - 1$ in $\mathbb{Z}_p$. Observe that the set of $(p-1)$-th roots of unity form a complete set of representatives of $\mathbb{Z}_p/p\mathbb{Z}_p$

Proposition 2.13. *The group of roots of unity $\mu(\mathbb{Q}_p)$ in $\mathbb{Q}_p$ is isomorphic to:*
i) $\mathbb{Z}/(p-1)\mathbb{Z}$, if $p \neq 2$.
ii) $\mathbb{Z}/2\mathbb{Z}$, if $p = 2$.

Proof. For $p \neq 2$, we need to prove that the reduction morphism $\epsilon : \mu(\mathbb{Q}_p) \to \mathbb{F}_p^*$ is bijective. We have already seen it is surjective. Suppose ζ is an n-th root of unity with $\zeta = 1 + pt \in \ker(\epsilon)$, with $t \in \mathbb{Z}_p$. We must have:

$$\zeta^n = (1+pt)^n = 1.$$

Hence, expanding the expression we get:

$$pt\left(n + \binom{n}{2}pt + \cdots + p^{n-1}t^{n-1}\right).$$

If $p \nmid n$, the term in parenthesis cannot be 0, and so $t = 0$. Therefore, if $t \neq 0$, necessarily $p \mid n$. We can replace ζ by ζ^p and n by n/p in the previous computation, and we arrive to $p^2 \mid n$. Repeating this argument we arrive to the case when $n = p$, which yields:

$$t\left(p + \binom{p}{2}pt + \cdots + p^{n-1}t^{n-1}\right) = t(p + p^2(\cdots)),$$

since $p \geq 3$. We cannot have $p + p^2(\cdots) = 0$, so we arrive at a contradiction, and t must be equal to 0. In conclusion, $\zeta = 1$.

For $p = 2$, we clearly have $\pm 1 \subseteq \mathbb{Z}_2^*$. We won't have any primitive 4-th root of unity, since if $\alpha \in \mathbb{Z}_2$ were one, we would have $\alpha^2 = -1$. But reducing modulo $2^2 = 4$, we would get a square root of 3 in $\mathbb{Z}/4\mathbb{Z}$, which doesn't exist. Arguing as above, if ζ is an n-th root of unity, with n prime to 2, we see that $\zeta = 1$. □

We can also use Hensel's lemma to study the squares of $\mathbb{Q}_p^*$. In the proof of the Kronecker-Weber theorem, and more particularly in the case of an extension of degree a power of 2, we use the next result.

Proposition 2.14. $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \cong (\mathbb{Z}/2\mathbb{Z})^3$.

Proof. Let $\alpha = p^r u \in \mathbb{Q}_2^*$. Clearly α will be a square if and only if $r = 2s$ for some s and $u \in \mathbb{Z}_2^{*2}$. Let $2^{\mathbb{Z}}$ denote the set of integral powers of 2. We have:

$$\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \cong (2^{\mathbb{Z}}/2^{2\mathbb{Z}}) \times (\mathbb{Z}_2^*/\mathbb{Z}_2^{*2}).$$

Clearly, $(2^{\mathbb{Z}}/2^{2\mathbb{Z}}) \cong \mathbb{Z}/2\mathbb{Z})$, so we only need to study $\mathbb{Z}_2^*/\mathbb{Z}_2^{*2}$.

Let's see that $\mathbb{Z}_2^{*2} = 1 + 2^3\mathbb{Z}_2$. Let $a \in \mathbb{Z}_2^{*2}$. Clearly $\mathbb{Z}_2^* = 1 + 2\mathbb{Z}_2$, so there exists some $b = 1 + 2c \in \mathbb{Z}_2^*$ such that $a = b^2$. We have $a = b^2 = 1 + 4(c + c^2)$. Since $c - c^2 = c(c-1)$, its reduction modulo 2 will be 0, and so $c \equiv c^2 \pmod 2$. Therefore, we have:

$$a = 1 + 4(c + c^2) = 1 + 4(2c + 2d) = 1 + 8(c + d) \in 1 + 8\mathbb{Z}_2.$$

On the other hand, if $a \in 1 + 8\mathbb{Z}_2$, we can apply Hensel's lemma to $f(X) = X^2 - a$, starting from the approximate solution $x = 1$. This is possible because we have $f(1) \equiv 0 \pmod{2^3}$ and $v_2(f'(1)) = v_2(2) = 1 < 3/2$. Hence, there is an element $b \in \mathbb{Z}_2$ with $b^2 = a$, as we wanted.

We can write $\mathbb{Z}_2^* = 1 + 2\mathbb{Z}_2$ as $\{\pm 1\} \times (1 + 4\mathbb{Z}_2)$, and so:

$$(\mathbb{Z}_2^*/\mathbb{Z}_2^{*2}) \cong \{\pm 1\} \times (1 + 4\mathbb{Z}_2)/(1 + 8\mathbb{Z}_2) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

In conclusion, we get the desired result:

$$\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

□

2.4 p-adic Analysis

We have seen that $\mathbb{Q}_p$ is a complete metric space, so we can consider the concepts of convergence of sequences and series of p-adic numbers. In this section we see that things work much differently for $\mathbb{Q}_p$ than they do for $\mathbb{R}$ or $\mathbb{C}$. The first results hold for non-archimedean valued fields in general.

Proposition 2.15. *A sequence $(a_n)_{n\geq 1}$ in a non-archimedean valued field is a Cauchy sequence if and only if $|a_{n+1} - a_n| \to 0$ as $n \to \infty$.*

Proof. If $(a_n)_{n\geq 1}$ is a Cauchy sequence, clearly $|a_{n+1} - a_n| \to 0$ as $n \to \infty$. Now suppose that for every $\epsilon > 0$, there exists $N > 0$ such that $|a_{n+1} - a_n| < \epsilon$, for $n \geq N$. Let $m \geq n \geq N$. Since the valuation is non-archimedean, we have that

$$|a_m - a_n| \leq \max_{n\leq i\leq m} |a_{i+1} - a_i| \leq \epsilon,$$

and so it is a Cauchy sequence. □

Proposition 2.16. *A series $\sum_{k=0}^{\infty} a_k$ in a complete non-archimedean valued field is convergent if and only if $a_k \to 0$ as $k \to \infty$.*

Proof. If the series converges, the a_n must tend to 0. Suppose that $a_n \to 0$. Consider the partial sums $s_k = \sum_{i=0}^{k} a_i$ and observe that $a_{k+1} = s_{k+1} - s_k$. Since $a_{k+1} \to 0$, by the previous proposition the partial sums will be a Cauchy sequence, and since the field is complete, it will converge. Hence, the series $\sum_{k=0}^{\infty} a_k$ converges. □

Since $\mathbb{Q}_p$ is a complete non-archimedean valued field, the previous result holds. Let's take a look at two basic power series, the logarithm and the exponential.

Definition 2.17. *We define the p-adic logarithm of $x \in \mathbb{Q}_p$ as the power series*

$$\log(1 + x) = \sum_{k\geq 1} (-1)^{k+1} \frac{x^k}{k},$$

and the p-adic exponential of x as

$$\exp(x) = \sum_{k\geq 0} \frac{x^k}{k!},$$

whenever they converge.

We have just taken the power series expansion of the classical logarithm and exponential for $\mathbb{R}$, and defined it for $\mathbb{Q}_p$. With this in mind, wherever these functions are defined, they will behave in the same way they do classically.

Just as in the classical case, power series have a radius of convergence, and to find this number for $\exp(x)$ we need to study the p-adic valuation of factorial numbers.

Lemma 2.18. *Let n be an integer and let $S_p(n)$ be the sum of the digits of n expressed in base p. Then,*

$$v_p(n!) = \frac{n - S_p(n)}{p - 1}.$$

Proof. We have $v_p(n!) = \sum_{1 \leq k \leq n} v_p(k)$. For a fixed k between 1 and n, consider its expansion in base p,

$$k = k_s p^s + \cdots + k_l p^l.$$

Here $l \geq s \geq 0$ and $k_s \neq 0$. Then we have:

$$k - 1 = p - 1 + (p-1)p + \cdots + (p-1)p^{s-1} + (k_s - 1)p^s + \cdots + k_l p^l.$$

Hence, $S_p(k-1) = s(p-1) + S_p(k) - 1$. Since $s = v_p(k)$, we get:

$$v_p(k) = \frac{1}{p-1}(1 + S_p(k-1) - S_p(k)).$$

Summing over all values between 1 and n, we get the telescoping sum:

$$v_p(n!) = \frac{1}{p-1} \sum_{1 \leq k \leq n} (1 + S_p(k-1) - S_p(k)) = \frac{1}{p-1}(n - S_p(n)),$$

proving the result.

□

Proposition 2.19. *The power series* $\exp(x)$ *converges precisely when* $|x| < |p|^{1/(p-1)}$, *and the power series* $\log(1+x)$ *converges precisely when* $|x| < 1$.

Proof. As we saw above, a p-adic series will converge if and only if its sequence of summands tends to 0. We will check the convergence using this characterization.

For the first series, observe that:

$$\left|\frac{x^k}{k!}\right| = |x|^k |p|^{-v_p(k!)} = |p|^{k v_p(x) - v_p(k!)}.$$

The exponent of the last term will be:

$$k\left(v_p(x) - \frac{1}{p-1}\right) + \frac{S_p(k)}{p-1}.$$

Since $S_p(k) \geq 0$ and $S_p(p^s) = 1$, the term on the left will determine the convergence of the series, and since $|p| < 1$, we have:

$$\left|\frac{x^k}{k!}\right| \to 0 \iff k\left(v_p(x) - \frac{1}{p-1}\right) \to \infty.$$

This will happen exactly when $v_p(x) > \frac{1}{p-1}$, equivalently when $|x| < |p|^{1/(p-1)}$.

Now consider the second power series. The condition $|x^k/k| \to 0$ implies $|x| < 1$, since $|k| = 1$ for all integers k prime to p. For every integer $k \geq 1$, we have that $1 \leq p^{v_p(k)} \leq k$, so $|k|^{-1} \leq k$. Hence, if $|x| < 1$, we have that

$$\left|\frac{x^k}{k}\right| \leq k|x|^k \to 0,$$

since $|x|^k$ beats the linearity of k.

□

3 Extensions of $\mathbb{Q}_p$ and Ramification Theory

In the previous chapter we studied the basic properties of $\mathbb{Q}_p$. Now we will study its finite extensions, and we will see that they are also local fields. After that, we will study their ramification behaviour. We follow chapter 2 of [Rob00] and chapter 5 of [Gou93]. At the end of the chapter we study completions of number fields and characterize them as finite extensions of $\mathbb{Q}_p$.

3.1 Finite Extensions of $\mathbb{Q}_p$

For the rest of this section, let K be a finite extension of $\mathbb{Q}_p$ of degree n. Our first objective is to find an absolute value on our field K that extends the p-adic absolute value on $\mathbb{Q}_p$. We can consider K as an n-dimensional vector space over $\mathbb{Q}_p$. We recall the definition of a norm on a vector space.

Definition 3.1. *Let k be a complete valued field (of characteristic zero) with absolute value $|\cdot|$. A **norm** on a k-vector space V is a function*

$$\|\cdot\| : V \to \mathbb{R}_+$$

that satisfies the following conditions:

1. *$\|x\| = 0$ if and only if $x = 0$.*
2. *for any $x \in V$ and any $\lambda \in k$, we have $\|\lambda x\| = |\lambda|\|x\|$.*
3. *$\forall x, y \in V$ we have $\|x + y\| \leq \|x\| + \|y\|$.*

The usual absolute value on $\mathbb{C}$ is a norm on $\mathbb{C}$, as well as its restriction on $\mathbb{R}$ is a norm on $\mathbb{R}$.

Any absolute value $|\cdot|_K$ on K that extends the p-adic absolute value ($|\cdot|_p$) on $\mathbb{Q}_p$ can be considered as a norm on the n-dimensional $\mathbb{Q}_p$ vector space K. Indeed, we have $|\lambda x|_K = |\lambda|_K|x|_K = |\lambda|_p|x|_K$ for every $\lambda \in \mathbb{Q}_p$ and $x \in K$. The other conditions are direct consequences of the definition of absolute value.

Definition 3.2. *Let V be a vector space over an absolute valued field k, two norms, $\|\cdot\|$ and $\|\cdot\|'$, are **equivalent** if they define the same topology on V. This happens exactly when there exist constants $C, c > 0$ such that for every $x \in V$,*

$$c\|x\| \leq \|x\|' \leq C\|x\|.$$

Proposition 3.3. *In a finite dimensional vector space V over a field k, all norms are equivalent. Furthermore, if the field k is a complete topological field, then V is also complete.*

We won't give a proof of this proposition here, but the interested reader can find a detailed exposition of this fact in sections 5.1 and 5.2 of [Gou93]. It is analogous to the case of $k = \mathbb{R}$, studied in the real analysis course given in the second year of degree.

Proposition 3.4. *For any finite extension K of $\mathbb{Q}_p$ there is at most one absolute value extending the p-adic absolute value.*

Proof. Suppose we have two absolute values $|\cdot|$ and $|\cdot|'$ on K. They can be considered as norms over K and therefore must be equivalent, since K is a finite vector space over $\mathbb{Q}_p$. Then there will exist $C, c > 0$ that satisfy $c|x| \leq |x|' \leq C|x|$ for every $x \in K$. Now, taking x^n instead of x yields the next inequality:

$$c|x^n| \leq |x^n|' \leq C|x^n|.$$

Since absolute values are multiplicative, we can write $|x^n| = |x|^n$. This gives us:

$$c|x|^n \leq |x|'^n \leq C|x|^n$$

Taking n-th roots, we have that for every $n \geq 0$ and every $x \in K$:

$$c^{1/n}|x| \leq |x|' \leq C^{1/n}|x|.$$

Letting $n \to \infty$, we have $c^{1/n} \to 1$ and $C^{1/n} \to 1$, so:

$$|x| \leq |x|' \leq |x|.$$

We conclude that $|x| = |x|'$ for every $x \in K$. □

Suppose that we have finite extensions $L/K/\mathbb{Q}_p$, with absolute values $|\cdot|_L$ and $|\cdot|_K$ extending the p-adic absolute value in $\mathbb{Q}_p$. Then the restriction of $|\cdot|_L$ to K yields an absolute value on K, and by the previous proposition, it must be equal to $|\cdot|_K$. So the absolute value of an element x doesn't depend on the context of x, and we simply write $|x|$ instead of $|x|_K$.

Now let's suppose K is a Galois extension over $\mathbb{Q}_p$ and assume the p-adic absolute value extends to K. We can define a new absolute value for every automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$ as $|x|' = |{}^\sigma x|$. It is easy to check that it is indeed an absolute value, and since σ induces the identity on $\mathbb{Q}_p$, it is also an extension of the p-adic absolute value on $\mathbb{Q}_p$. By the previous proposition, $|x| = |{}^\sigma x|,\ \forall \sigma \in G = \mathrm{Gal}(K/\mathbb{Q}_p)$. Let $\mathrm{N} = \mathrm{N}_{K/\mathbb{Q}_p}$ be the norm from K to $\mathbb{Q}_p$ (not to be confused with the vector space norm!). We saw in chapter 2 that for every $x \in K$ we have:

$$\mathrm{N}(x) = \prod_{\sigma \in G} {}^\sigma x \in \mathbb{Q}_p.$$

We must have:

$$|\mathrm{N}(x)| = \prod_{\sigma \in G} |{}^\sigma x| = \prod_{\sigma \in G} |x| = |x|^n.$$

Therefore, we can write:

$$|x| = |\mathrm{N}(x)|^{1/n}.$$

As $\mathrm{N}(x) \in \mathbb{Q}_p$, we have found an explicit expression of the absolute value on K, provided that one exists, in terms of the p-adic absolute value on $\mathbb{Q}_p$ and the norm function. To see this we have assumed that K is Galois over $\mathbb{Q}_p$, but the next lemma shows that this expression is well defined for every finite extension of $\mathbb{Q}_p$.

Lemma 3.5. *Let $K/L/\mathbb{Q}_p$ be a tower of finite field extensions. We set $n = [K : \mathbb{Q}_p]$ and $m = [L : \mathbb{Q}_p]$. Let $x \in L$, then:*

$$\sqrt[m]{|N_{L/\mathbb{Q}_p}(x)|_p} = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p}.$$

Proof. We have that

$$\mathrm{N}_{K/\mathbb{Q}_p}(x) = \mathrm{N}_{L/\mathbb{Q}_p}(\mathrm{N}_{K/L}(x)),\ \forall x \in K$$

and as $x \in L$, $\mathrm{N}_{K/L}(x) = x^{[K:L]}$. By the multiplicativity of the norm, we have that $\mathrm{N}_{K/\mathbb{Q}_p}(x) = \mathrm{N}_{L/\mathbb{Q}_p}(x)^{[K:L]}$. Since $[K : \mathbb{Q}_p] = [K : L][L : \mathbb{Q}_p]$, we conclude that:

$$|\mathrm{N}_{K/\mathbb{Q}_p}(x)|_p^{1/n} = |\mathrm{N}_{L/\mathbb{Q}_p}(x)|_p^{[K:L]/n} = |\mathrm{N}_{L/\mathbb{Q}_p}(x)|_p^{1/m}.$$

□

Let's use this observation to construct an extension of the p-adic absolute value in any finite extension K.

Proposition 3.6. *Let K be a finite extension $\mathbb{Q}_p$ of degree n. There exists a (unique) non-archimedean absolute value $|\cdot|$ on K extending the p-adic absolute value. For every $x \in K$, it is defined by the expression:*

$$|x| = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p}.$$

Proof. Let's check that $|\cdot|$ as defined above is indeed an absolute value.
First, observe that $|x| = 0$ if and only if $\mathrm{N}_{K/\mathbb{Q}_p}(x) = 0$, and this only happens when $x = 0$. Since $\mathrm{N}_{K/\mathbb{Q}_p}(xy) = \mathrm{N}_{K/\mathbb{Q}_p}(x)\mathrm{N}_{K/\mathbb{Q}_p}(y)$, we will also have that $|xy| = |x||y|$. For every $x \in \mathbb{Q}_p$, $\mathrm{N}_{K/\mathbb{Q}_p}(x) = x^n$, and therefore $|x| = |x|_p$, so it is an extension of the p-adic absolute value.

The hardest condition to check is the non-archimedean inequality, i.e., that for every $x, y \in K$, $|x + y| \leq \max\{|x|, |y|\}$. We can suppose $y \neq 0$, and dividing by y, all we need to show is:

$$|x + 1| \leq \max\{|x|, 1\}.$$

We only need to prove that $|x| \leq 1$ implies $|x - 1| \leq 1$. Suppose this were true, and take $x \in K$. If $|x| \leq 1$, then $|-x| \leq 1$ and so $|-x-1| = |x+1| \leq 1$. Since $\max\{|x|, 1\} = 1$, we are done. On the other hand, if $|x| > 1$, $|1/x| < 1$, and as we've just seen:

$$\left|\frac{x}{x+1}\right| = \left|1 + \frac{1}{x}\right| \leq 1.$$

Therefore $|x + 1| \leq |x|$, just as we wanted.

Now, by the definition of $|\cdot|$, we have that $|x| \leq 1$ happens exactly when $|\mathrm{N}_{K/\mathbb{Q}_p}(x)|_p \leq 1$. So what we want to show is that:

$$|\mathrm{N}_{K/\mathbb{Q}_p}(x)|_p \leq 1 \implies |\mathrm{N}_{K/\mathbb{Q}_p}(x - 1)|_p \leq 1.$$

Recalling the definition of $|\cdot|_p$, this can be written as:

$$\mathrm{N}_{K/\mathbb{Q}_p}(x) \in \mathbb{Z}_p \implies \mathrm{N}_{K/\mathbb{Q}_p}(x-1) \in \mathbb{Z}_p.$$

We shall see this using the definition of $\mathrm{N}_{K/\mathbb{Q}_p}(x)$ in terms of the minimal polynomial of x. By the previous lemma, we can assume $K = \mathbb{Q}_p(x)$. It is clear that $\mathbb{Q}_p(x) = \mathbb{Q}_p(x-1)$. Let $f(X)$ be the minimal polynomial for x. Let 's write it as:

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0.$$

The minimal polynomial for $x-1$ will be $f(X+1)$, since $f(x-1+1) = f(x) = 0$, it is monic and $\deg(f(X+1)) = n$. We can write it as:

$$f(X+1) = X^n + \cdots + (1 + a_{n-1} + \cdots + a_1 + a_0),$$

where the number in parenthesis is the constant coefficient.

Therefore, we have that $\mathrm{N}_{K/\mathbb{Q}_p}(x) = (-1)^n a_0$ and also that $\mathrm{N}_{K/\mathbb{Q}_p}(x-1) = (-1)^n(1 + a_{n-1} + \cdots + a_1 + a_0)$. So what we need to prove is:

$$a_o \in \mathbb{Z}_p \implies (1 + a_{n-1} + \cdots + a_1 + a_0) \in \mathbb{Z}_p.$$

We will prove something that is even stronger.

Lemma 3.7. *Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Q}_p[X]$ be a monic irreducible polynomial, with constant coefficient $a_0 \in \mathbb{Z}_p$. Then, all the coefficients of $f(X)$ are in $\mathbb{Z}_p$.*

Proof. We will prove that if any of the coefficients is not in $\mathbb{Z}_p$, then $f(X)$ is reducible. Suppose some $a_i \notin \mathbb{Z}_p$. Let m be the smallest integer such that $p^m a_i \in \mathbb{Z}_p$, for every $i = 1, \ldots, n$. Then we have $g(x) = p^m f(X) \in \mathbb{Z}_p$. We can write it as:

$$g(x) = b_n X^n + \cdots + b_1 X + b_0,$$

where each $b_i = p^m a_i$.

Since $f(X)$ is monic, we have $b_n = p^m$ and it will be divisible by p. $b_0 = p^m a_0$ will also be divisible by p, since $a_0 \in \mathbb{Z}_p$. By our choice of m, there will be at least one b_i which is not divisible by p. Let's denote by k the smallest integer such that b_k is not divisible by p. Then we will have a factorization of $g(X)$ modulo p.

$$g(X) \equiv (X^{n-k} + \cdots + b_k)X^k \pmod{p}$$

and clearly both factors are relatively prime modulo p. By the second form of Hensel's lemma, $g(X) = p^m f(X)$ must be reducible, and therefore $f(X)$ will also be reducible, contradicting the assumptions of the theorem. Therefore, all the coefficients live in $\mathbb{Z}_p$

□

We conclude that all the a_i are in $\mathbb{Z}_p$, and so $1 + a_{n-1} + \cdots + a_1 + a_0 \in \mathbb{Z}_p$, as we wanted to see. $\square$

In conclusion, any finite extension K of $\mathbb{Q}_p$ is a complete non-archimedean valued field.

Moreover, we can see that the absolute value comes from a valuation on K. We have that:

$$|x| = |\mathrm{N}_{K/\mathbb{Q}_p}(x)|_p^{1/n} = p^{-v_p(\mathrm{N}_{K/\mathbb{Q}_p}(x))/n}, \ \forall x \in K.$$

So for $x \in K$ we can define its valuation as

$$v_p(x) = \frac{1}{n} v_p(\mathrm{N}_{K/\mathbb{Q}_p}(x)).$$

Observe that $v_p(x) \geq 0 \iff |x| \leq 1$, so we can consider the ring of integers of K:

$$\mathcal{O}_K = \{\alpha \in K : |x| \leq 1\},$$

with maximal ideal:

$$\mathfrak{p}_K = \{\alpha \in K : |x| < 1\}.$$

As we saw in chapter 2, $\mathcal{O}_K$ will be a discrete valuation ring, and so it will also be a Dedekind Domain. Therefore we can consider the ramification index and the residue field degree of p in $\mathcal{O}_K$, and as we only have one prime ideal in $\mathcal{O}_K$, we will write them as e and f, respectively.

The residue field $k = \mathcal{O}_K/\mathfrak{p}_K$ will be a finite extension of $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$, and so $k \cong \mathbb{F}_q$ the (unique) finite field with q elements, where $q = p^f$. Since the residue field is finite and K is complete, by proposition 2.7 we have that K will be a local field.

Let $\pi \in \mathfrak{p}_K$ be an element of maximum absolute value, equivalently of minimum valuation. Then π generates $\mathfrak{p}_K$, since for every $x \in \mathfrak{p}_K$ we have $|x| \leq |\pi|$ and so $x/\pi \in \mathfrak{p}_K$. So we can write every $x \in \mathfrak{p}_K$ as $x = \pi^m u$, for some $m \geq 1$ and some unit $u \in \mathcal{O}_K$. Therefore, $v_p(x) = m v_p(\pi)$, and since π will have minimum valuation, the image of v will be $\frac{1}{v(\pi)}\mathbb{Z}$. Now, recall that $p = \pi^e$, so $v_p(\pi) = v_p(p)/e = 1/e$. With this we conclude that the image of v_p is:

$$v_p(\mathcal{O}_K) = \frac{1}{e}\mathbb{Z}.$$

For $\pi \in \mathcal{O}_K$, $|\pi|^e = |p| \iff \pi$ is a prime element of $\mathcal{O}_K$. We shall refer to any such element as a ***uniformizer*** of K.

Let $S \subseteq \mathcal{O}_K$ be a complete set of representatives for the classes of the residue field of K, containing 0, and let π be a uniformizer of K. Then for each element $x \in \mathcal{O}_K$, there is a unique $a_0 \in S$ such that $x - a_0 \in (\pi)$. For some $x_1 \in \mathcal{O}_K$ we can write:

$$x = a_0 + \pi x_1.$$

Repeating this procedure we get that for some x_{n+1} :

$$x = \sum_{i=0}^{n} a_i \pi^i + x_{n+1} = s_n + x_{n+1}.$$

Since $|x_n\pi^n| \leq |\pi^n| \to 0$, the partial sums $(s_n)_{n\geq 1}$ form a Cauchy sequence that converge to x. Therefore, we can express each $x \in \mathcal{O}_K$ a power series of π with coefficients in S:

$$\sum_{i\geq 0} a_i\pi^i.$$

We can extrapolate this to elements $\alpha \in K$, taking also negative powers of π. Then we would have that $i \geq m$, for some $m \in \mathbb{Z}$.

We refresh the definitions we gave for ramification of ideals and extend it to fields.

Definition 3.8. *Let L/K be finite extension of $\mathbb{Q}_p$, with $n = [L : K]$, and let $\mathfrak{p}_L$ and $\mathfrak{p}_K$ be its respective prime ideals. Let $e_{L/K}$ and $f_{L/K}$ be the ramification index and residue field degree of $\mathfrak{p}_K$ in L. We say that L/K is:*

1. ***unramified*** *when $e_{L/K} = 1$, i.e. $f_{L/K} = n$.*
2. ***totally ramified*** *when $f_{L/K} = 1$, i.e. $e_{L/K} = n$.*
3. ***tamely ramified*** *when p does not divide $e_{L/K}$.*
4. ***wildly ramified*** *when $e_{L/K}$ is a power of p.*

In other words, L is unramified over K if any uniformizer of K is a generator of $\mathfrak{q}_L \subseteq \mathcal{O}_L$; L is totally ramified when the residue field does not grow in the extension.

Proposition 3.9 (Hensel's Lemma)**.** *Let K be a finite extension of $\mathbb{Q}_p$, and let $f(X) \in \mathcal{O}_K[X]$. If $x \in \mathcal{O}_K$ satisfies:*

$$|f(x)| < |f'(x)|^2,$$

then there is a unique root $\xi \in \mathcal{O}_K$ of $f(X)$ such that $|\xi - x| = |f(x)/f'(x)| < |f'(x)|$.

The proof is exactly the same as the one for the case $K = \mathbb{Q}_p$.

3.2 Totally Ramified Extensions

In this section we will study the structure of totally ramified extensions L/K over $\mathbb{Q}_p$. First, let's remind some lemmas on polynomials.

Lemma 3.10 (Eisenstein's Criterion)**.** *Let A be a UFD with field of fractions K. Let:*

$$f(X) = a_nX^n + \cdots + a_1X + a_0,\ a_i \in A[X];$$

Suppose there is a prime $\pi \in A$ such that:
i) $\pi \mid a_i$, for $i = 0, \ldots, n-1$.
ii) $\pi \nmid a_n$.
iii) $\pi^2 \nmid a_0$.
Then $f(X)$ is irreducible in $K[X]$.

Any polynomial that satisfies this conditions will be called an ***Eisenstein polynomial***, or a π-Eisenstein polynomial, and will be irreducible as stated in the lemma.

Proposition 3.11. *Let $K/\mathbb{Q}_p$ be a finite extension of degree $n = [K : \mathbb{Q}_p]$. Then, $K/\mathbb{Q}_p$ is totally ramified if and only if $K = \mathbb{Q}_p(\pi)$, where π is is a root of an Eisenstein polynomial. Futhermore, π will be a uniformizer of K.*

Proof. Let $f(X) \in \mathbb{Q}_p[X]$ be an Eisenstein polynomial of degree n, and consider $K = \mathbb{Q}_p(\pi)$, where π is a root of $f(X)$. Let's calculate the valuation of π in $\mathcal{O}_K$:

$$v_p(\pi) = \frac{1}{n} v_p(\mathrm{N}_{K/\mathbb{Q}_p}(\pi)) = \frac{1}{n} v_p(a_0).$$

Since a_0 is the constant coeficient of an p-Einsenstein polynomial, we will have $v_p(a_0) = 1$, and so $v_p(\pi) = 1/n$. Therefore, the ramfication index e will be equal to the degree of the field extension, n, so K is indeed totally ramified over $\mathbb{Q}_p$ and π is a uniformizer of K.

Now suppose that $K/\mathbb{Q}_p$ is a totally ramified extension. Let π be a uniformizer of K. We will have that $v_p(\pi) = 1/n$. Let $f(X) \in \mathbb{Q}_p$ be the minimal polynomial of π over $\mathbb{Q}_p$, of degree s. Now, we can compute the norm of π taking a_0 as the constant coeficient of f: $\mathrm{N}_{K/\mathbb{Q}_p}(\pi) = (-1)^n a_0^{n/s}$. Therefore,

$$p^{-1/n} = |\pi| = \sqrt[n]{|a_0^{n/s}|} = |a_0|^{1/s}.$$

Since $a_0 \in \mathbb{Q}_p$, its absolute value will be an integral power of p, $|a_0| = p^t$. Hence, we must have $s = nt$, and since $0 < s \leq n$, we conclude that $s = n$ and $t = -1$.

Thus, the degree of $f(X)$ will be equal to $[K : \mathbb{Q}_p]$, which proves $K = \mathbb{Q}_p(\pi)$. We have already seen that $|a_0| = p^{-1}$, and since $f(X)$ is monic, we also have that $p \nmid a_n$. We only need to check that all the other coefficients of $f(X)$ satisfy $|a_i| < 1$.

Consider $\pi_1, \ldots, \pi_n$, the roots of $f(X)$ in some splitting field over K. Since they all have the same minimal polynomial, they will all have the same norm and the same absolute value. In particular, $|\pi_i| < 1$. We can write $f(X)$ as:

$$f(X) = \prod_{i=1}^{n} (X - \pi_i).$$

If we expand this expression we get that for $0 < i < n$, a_i will be a sum of products of $n - i$ of the π_j. As we saw in chapter 1, in a non-archimedean valued field the absolute value of a sum is smaller or equal to the maximum of the absolute values of the summands. So $|a_i| \leq |\pi_{j_1} \pi_{j_2} \cdots \pi_{j_{n-i}}| = |\pi|^{n-i} < 1$. We conclude that $f(x)$ is an Eisenstein polynomial, just as we wanted to see. □

The next lemma is a nice example of a totally ramified extension of $\mathbb{Q}_p$, and it also useful in the proof of the Kronecker-Weber theorem.

Lemma 3.12. *For any prime p we have $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p((-p)^{1/(p-1)})$, and it is a totally ramified extension over $\mathbb{Q}_p$*

Proof. Let's recall that ζ_p is a root of the p-th cyclotomic polynomial $\Phi_p(X)$:

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

$\Phi_p(X)$ is irreducible, since the change of variables $Y = X - 1$ produces a p-Eisenstein polynomial:

$$\Phi_p(X + 1) = X^{p-1} + pX^{p-2} + \cdots + p.$$

By the previous proposition, $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\zeta_p - 1)$ is a totally ramified extension, of degree $p - 1$, with uniformizer $\pi = \zeta_p - 1$.

Now, consider $\alpha = (-p)^{1/(p-1)}$. It is a root of the p-Eisenstein polynomial $X^{p-1}+p$, and so $\mathbb{Q}_p(\alpha)$ is a totally ramified extension of degree $p - 1$. We shall see that $\alpha \in \mathbb{Q}_p(\zeta_p)$, and since $\mathbb{Q}_p(\alpha)$ and $\mathbb{Q}_p(\zeta_p)$ have the same degree over $\mathbb{Q}_p$, both fields will be equal.

We know that $\pi^{p-1} = -p(\pi^{p-2} + \cdots + 1)$, so we will have that $u := -\pi^{p-1}/p \equiv 1 \pmod{\pi}$. Therefore, u will be a unit in the ring $\mathcal{O}_K$. Let $g(X) = X^{p-1} - u \in K[X]$. We have $g(1) \equiv 0 \pmod{\pi}$ and $g'(1) = p - 1 \not\equiv 0 \pmod{\pi}$, so by Hensel's lemma, we can lift 1 to a root $\beta \in \mathbb{Q}_p(\zeta_p)$ of $g(X)$.

Now, we have that $p\beta^{p-1} = pu = -\pi^{p-1}$, so $(\pi/\beta)^{p-1} + p = 0$. Since $\mathbb{Q}_p(\zeta_p)$ is a Galois extension of $\mathbb{Q}_p$ and $\pi/\beta \in \mathbb{Q}_p(\zeta_p)$, every root of the mynimal polynomial of π/β also lives in $\mathbb{Q}_p(\zeta_p)$. In particular, $\alpha \in \mathbb{Q}_p(\zeta_p)$, as we wanted. □

We saw in the section 3.1 that every finite (hence algebraic) extension of $\mathbb{Q}_p$ there is a unique extension of the p-adic absolute value. So for every element α in the maximal algebraic extension of $\mathbb{Q}_p$, $\mathbb{Q}_p^{al}$, we can define its absolute value as the absolute value of a in $\mathbb{Q}_p(a) \subseteq \mathbb{Q}_p^{al}$. It is well defined, since for any two finite extensions of $\mathbb{Q}_p$, their respective absolute values must agree on their intersection, and so $|a|$ does not depend on the field it is contained in.

Theorem 3.13 (Krasner's Lemma)**.** *Let K be a finite extension of $\mathbb{Q}_p$. Let $a \in \mathbb{Q}_p^{al}$. Let's denote by $a = a_1, a_2, \ldots, a_n$ the conjugates of a over K. Suppose that $b \in \mathbb{Q}_p^{al}$ is closer to a than a is to any of its conjugates:*

$$|a - b| < |a - a_i|, \ \forall i = 2, \ldots, n.$$

Then, $K(a) \subseteq K(b)$.

Proof. Let $L = K(b)$, and suppose $a \notin L$. Then, $[L(a) : L] = m > 1$. Since the characteristic of K is 0, the degree of an extension is equal to its separability degree. Therefore, there must exist m different homomorphisms $\sigma : L(a) \to \bar{K}$ that fix the field L. In particular, they fix the field K and hence send a to one of its conjugates over K. By our assumption, $a \notin L$, so there will be at least one of these morphisms that doesn't fix a. Let's denote it by σ_0.

Now, since σ_0 fixes $b \in L$, we will have:

$$|\sigma_0(a) - b| = |\sigma_0(a) - \sigma_0(b)| = |\sigma_0(a - b)| = |a - b|.$$

This implies

$$|a - \sigma_0(a)| \leq \max(|a - b|, |b - \sigma_0(a)|) = |a - b|,$$

which is a clear contradiction with the assumption that b was closer to a than any of its conjugates. Therefore, our assumption was wrong and $a \in L$. So $K(a) \subseteq K(b)$. $\square$

Krasner's Lemma has a very interesting although rather technical corollary.

Definition 3.14. *Let K be a finite extension of $\mathbb{Q}_p$. Let $f \in K[X]$, with coefficients $f_i \in K$. We define its L^1 norm on $K[X]$ as:*

$$\|f\|_1 := \sum_i |f_i|.$$

Proposition 3.15. *Let $K/\mathbb{Q}_p$ be a finite extension, and let $f \in K[X]$ be a monic irreducible polynomial. Then there exists $\delta > 0$ such that for every monic polynomial $g \in K[X]$ with $\|f - g\|_1 < \delta$, every root β of g has a corresponding root α of f such that:*

$$K(\alpha) = K(\beta).$$

In particular, g will be irreducible.

Another use for Krasner's lemma is the next proposition, that gives us the structure of tamely ramified extensions of $\mathbb{Q}_p$.

Proposition 3.16. *Let L/K be finite extensions of $\mathbb{Q}_p$. Suppose L/K is totally and tamely ramified of degree e. Then there exists $\pi \in K$, a generator of $\mathfrak{p}_K$ such that $L = K(\pi^{1/e})$.*

Proof. Consider π_K and π_L, uniformizers of K and L respectively. Since the extension is totally ramified, we have $|\pi_L|^e = |\pi_K|$ and so $\pi_L^e/\pi_K = u$ is a unit in $\mathcal{O}_L$. Now, since the residue fields are the same for both extensions, we can take $\zeta \in \mathcal{O}_K^*$ such that $\zeta \equiv u \pmod{\pi_L}$. Hence, for some $v' \in \mathcal{O}_L$, we have:

$$\pi_L^e = \pi_K u, \ u = \zeta + \pi_L v'.$$

This yields

$$\pi_L^e = \pi_K \zeta + \pi_K \pi_L v'.$$

The element $\zeta \pi_K$ is also a generator of the ideal $\mathfrak{p}_K$, so we can forget about our original choice of uniformizer and rename this new element as π_K. Therefore, we have that for some $v \in \mathcal{O}_L$:

$$\pi_L^e = \pi_K + \pi_K \pi_L v.$$

Now consider the polynomial $f(X) = X^e - \pi_K$. It is an π_K-Eisenstein polynomial, and hence irreducible over $\mathcal{O}_K[X]$. We have $f(\pi_L) = \pi_K \pi_L v$, which implies that $|f(\pi_L)| = |\pi_K \pi_L v| < |\pi_K|$.

Let $\alpha_1, \ldots, \alpha_e$ be the roots of $f(X)$ in some splitting field over K. Since $f(X)$ is irreducible, the α_i are conjugate and therefore have the same absolute value. We also

have that $\prod \alpha_i = \pi_K$, the constant coeficient of $f(X)$, and so $|\alpha_i| = |\pi_K|^{1/e} = |\pi_L|$. From this we get that for every i

$$|\pi_L - \alpha_i| \leq \max(|\alpha_i|, |\pi_L|) = |\pi_L|.$$

But we also have that $\prod |\pi_L - \alpha_i| = |f(\pi_L)| < |\pi_K|$, so at least one of the factors is smaller than $|\pi_L|$. Let's suppose we have $|\pi_L - \alpha_1| < |\pi_L|$.

On the other hand, for every $i \neq 1$ we have that $|\alpha_i - \alpha_1| \leq \max(|\alpha_i|, |\alpha_1|) = |\alpha_1|$. Since $p \nmid e$(the extension is tamely ramified) we have

$$\prod_{i \neq 1} |\alpha_i - \alpha_1| = |f'(\alpha_1)| = |e\alpha_1^{e-1}| = |\alpha_1|^{e-1}.$$

From this we can conclude that $|\alpha_i - \alpha_1| = |\alpha_1| = |\pi_L|$.

So π_L is closer to α_1 than any of its conjugates, and by Kranser's lemma we get that

$$K(\alpha_1) \subseteq K(\pi_L) \subseteq L$$

Since $[K(\alpha_1) : K] = e = [L : K]$, we conclude that $K(\alpha_1) = L$, just as we wanted to see.

□

3.3 Unramified Extensions

Unramified extensions of $\mathbb{Q}_p$ are much simpler to characterize than totally ramified ones. As a matter of fact, they are always cyclotomic extensions. Let's denote the residue fields of K and L by k and l respectively.

Theorem 3.17. *Let L/K be finite extensions of $\mathbb{Q}_p$. Then there is a bijection between:*

$$\{K' \subseteq L \mid K' \text{ unramified over } K\} \longleftrightarrow \{k' \subseteq l \mid k' \text{ finite over } k\}$$

Moreover, $K' \subseteq L$ is unramified over K with degree n if and only if $K' = K(\zeta_{q^n-1})$, where $q = |k|$.

Proof. Let k' be finite extension of k contained in l. Since k is a finite field, there will exist an $a \in k'$ such that $k' = k(a)$. Let $\tilde{f}$ be the minimal polynomial of a over k, and let $f \in K[X]$ be a monic lift of $\tilde{f}$. f will be irreducible and have the same degree as $\tilde{f}$. Since a is a simple root of $\tilde{f}$ (every finite field is separable) we have that $\tilde{f}'(a) \neq 0$. Therefore, for any lift $x \in \mathcal{O}_L$ of a, $|f'(x)|^2 = 1 > |f(x)|$ and we can apply Hensel's lemma. Let $\alpha \in L$ be the unique root of f congruent to a mod $\mathfrak{p}_L$. Now lets see that $K' = K(\alpha)$ is an unramified extension of K with residue field k'.

Let n be the degree of $\tilde{f}$, $\tilde{k}$ the residue field of K'. Since $\alpha \in K'$, we'll have $a \in \tilde{k}$ and $k' \subseteq \tilde{k}$. Now, $[\tilde{k} : k] \leq [K' : K] = n$ and $n = [k' : k] \leq [\tilde{k} : k]$. Therefore, these are all equalities and we have that $\tilde{k} = k'$ and $[K' : K] = [k' : k]$, exactly as we wanted to see.

Observe that since a generates k' over $k = \mathbb{F}_q$, a will be a $(q^n - 1)$-th root of unity, with $n = [K' : K] = [k' : k]$. Therefore, α will also be a $(q^n - 1)$-th root of unity. So $K' = K(\zeta_{q^n-1})$.

Now suppose that K'/K is an unramified extension of degree n, $K' \subseteq L$. As we have just seen, there will be an $(q^n - 1)$-th root of unity generating k' over k, and we can lift it to a $\zeta_{q^n-1} \in K'$. But we've also seen that $[K(\zeta_{q^n-1}) : K] = n = [K' : K]$, so $K' = K(\zeta_{q^n-1})$.

In conclusion, $K' \subseteq L$ is unramified over K with degree n if and only if $K' = K(\zeta_{q^n-1})$.

□

As a corollary, every finite extension L/K has maximal unramified extension of K in L. We denote it by K^{unr}, and by the propostion it will be equal to $K(\zeta_{q^f-1})$, where f is the residue class degree of L over K and $q = |k|$. We have that $[K^{unr} : K] = f$, so the extension L/K^{unr} is totally ramified. Observe too that unramified extensions are cyclotomic, and hence will always be Galois.

Corollary 3.18. *Let $K/\mathbb{Q}_p$ be a finite extension, with residue degree f. Then, K contains a primitive $(p^f - 1)$-th root of unity.*

Suppose we are in the situation were L is Galois over K. We've already seen that conjugates have the same absolute value, so every element $\sigma \in G = \mathrm{Gal}\,(L/K)$ preseves $\mathcal{O}_L$ and $\mathfrak{p}_L$. Therefore, every $\sigma \in G$ acts in a well defined way over $l = \mathcal{O}_L/\mathfrak{p}_L$. So we can define the morphism

$$\varphi : G \to \mathrm{Gal}(l/k).$$

Proposition 3.19. *The morphism φ is an epimorphism.*

Proof. Let's denote by $\tilde{\sigma}$ the image of σ by φ. Obviously, the identity in $\mathrm{Gal}(L/K)$ is mapped to the identity in $\mathrm{Gal}(l/k)$. We know that, since l/k is a finite extension of finite groups, its Galois group will be cyclic and generated by the Frobenius element. All we need to check is that Frobenius element is in the image of φ.
Since l/k is a finite separable extension, we can choose a primitive element $a \in l$ such that $l = k(a)$. Let's fix an $\alpha \in L$ such that $\alpha \equiv a \pmod{\mathfrak{p}_L}$. Its minimal polynomial over K will be $f(X) = \prod_{\sigma \in G} (X - \sigma(\alpha)) \in K[X]$. Therefore, when we reduce it we get a polynomial with coeficients in k

$$\tilde{f}(X) = \prod_{\sigma \in G} \left(X - \tilde{\sigma}(a)\right).$$

Since $\mathrm{Id} \in G$, a will be one of the roots of $\tilde{f}$. Therefore, the minimal polynomial of a over k will divide $\tilde{f}$, and so all the conjugates of a will be roots of $\tilde{f}$. In particular, $\mathrm{Frob}(a)$ will be a root of $\tilde{f}$, and so it must be the image of some $\sigma \in G$. We can conclude that $\mathrm{Frob} \in \mathrm{Im}(\varphi)$, and that φ is surjective. □

Definition 3.20. *Inertia group, $I_{\mathfrak{p}_L} = I_{\mathfrak{p}_L}(l/K)$, is the kernel of the map φ.*

In particular, we have the next corol·lary.

Corollary 3.21. *We have* $\mathrm{Gal}(L/K)/I_{\mathfrak{p}_L} \cong \mathrm{Gal}(l/k)$ *and the order of the inertia group is equal to the ramification index of* L/K*, i.e.* $|I_{\mathfrak{p}_L}| = e_{L/K}$.

Proof. The first part is obvious by the first isomorphism theorem. Since the order of $\mathrm{Gal}(l/k) = f_{L/K}$ and the order of $\mathrm{Gal}(L/K) = n = e_{L/K} f_{L/K}$, we must have $|I_{\mathfrak{p}_L}| = n/f_{L/K} = e_{L/K}$. □

Corollary 3.22. L/K *is unramified if and only if* $I_{\mathfrak{p}_L} = (1)$*, and in this case, we have that* $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(l/k)$ *is cyclic.*

3.4 Completions of Global Fields

We saw in chapter 2 that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic absolute value. In this subsection, we see that the completion of every finite extension K of $\mathbb{Q}$ with respect to some prime $\mathfrak{p}$ lying over p is a finite extension of $\mathbb{Q}_p$, and reciprocally that finite extensions of $\mathbb{Q}_p$ are completions of number fields with respect to primes lying over p. These results are the key for the local-global principle to work for the Kronecker-Weber theorem. We follow lecture 11 of [Sut17].

Let $L/K/\mathbb{Q}$ be finite extensions. Let $\mathcal{O}_K \subseteq \mathcal{O}_L$ be the ring of integers of K and L respectively. In particular, $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$. Since both rings are Dedekind Domains, $\mathfrak{p}\mathcal{O}_L$ can be written as a product of prime ideals of $\mathcal{O}_L$:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}.$$

Each prime ideal $\mathfrak{q}$ of the ring of integers of a number field L defines an absolute value on L. First consider the localization of $\mathcal{O}_L$ with respect to $\mathfrak{q}$, $\mathcal{O}_\mathfrak{q}$. We know by Proposition 1.12 that $\mathcal{O}_\mathfrak{q}$ is a DVR, so we can consider the valuation it defines on L: $v_\mathfrak{q}$. The ideal $\mathfrak{q}$ lies over $\mathfrak{q} \cap \mathbb{Z}$, a prime ideal in $\mathbb{Z}$. Hence, $\mathfrak{q} \cap \mathbb{Z} = (p)$ for some prime integer p. Let $e_{\mathfrak{q}/p}$ be ramification index of $\mathfrak{q}$ over p. We define the $\mathfrak{q}$-adic absolute value on L as :

$$|a|_\mathfrak{q} := p^{-v_\mathfrak{q}(a)/e_{\mathfrak{q}/p}}, \ \forall a \in L^*.$$

We have that for every $\alpha \in \mathbb{Q}$, $v_\mathfrak{q}(\alpha) = e_{\mathfrak{q}/p} v_p(\alpha)$. We say that the valuation $v_\mathfrak{q}$ ***extends*** v_p ***with index*** $e_{\mathfrak{q}/p}$. From this we see that $|\cdot|_\mathfrak{q}$ extends the p-adic absolute value on $\mathbb{Q}$. In the same way, for every prime $\mathfrak{p}$ in $\mathcal{O}_K$ such that $\mathfrak{q} \mid \mathfrak{p}$, the $\mathfrak{q}$-adic absolute value extends the $\mathfrak{p}$-adic absolute value, since $v_\mathfrak{q}$ extends $v_\mathfrak{p}$ with index $e_{\mathfrak{q}/\mathfrak{p}}$ and $e_{\mathfrak{q}/p} = e_{\mathfrak{q}/\mathfrak{p}} \cdot e_{\mathfrak{p}/p}$.

Let $L_\mathfrak{q}$ be the completion of L with respect to $\mathfrak{q}$, i.e. with respect to $|\cdot|_\mathfrak{q}$; and let $K_\mathfrak{p}$ be the completion of K with respect to $\mathfrak{p}$. Since $|\cdot|_\mathfrak{q}$ extends $|\cdot|_\mathfrak{p}$ and $L_\mathfrak{q}$ is complete and contains K, it will also contain $K_\mathfrak{p}$. Moreover, we have that both $L_\mathfrak{q}$ and $K_\mathfrak{p}$ are extensions of $\mathbb{Q}_p$. The next proposition assures us that these extensions are finite.

Proposition 3.23. *If L/K are finite extensions of number fields, then their completions with respect to the primes $\mathfrak{q} \mid \mathfrak{p}$, $L_\mathfrak{q}/K_\mathfrak{p}$, are also finite extensions, with $[L_\mathfrak{q} : K_\mathfrak{p}] \leq [L : K]$.*

Proof. Let $n = [L : K]$ and let $b_1, \ldots, b_n \in L$ be a K-basis of L. By the definition of completion of a metric field, we can view each element of $L_\mathfrak{q}$ as a Cauchy sequence of elements of L. So let $(y_m)_{m\geq 1}$ be a Cauchy sequence in L. Each y_m can be written as $y_m = x_{m,1}b_1 + \cdots + x_{m,1}b_n$ for some $x_{m,i} \in K$. Therefore, we can write:

$$(y_m)_{m\geq} = (x_{m,1})_{m\geq 1}b_1 + \cdots + (x_{m,n})_{m\geq 1}b_n.$$

The mapping from L to K that sends each y_m to its i-th component is a linear mapping between finite dimensional normed vector spaces, and hence continuous. Therefore, it will send Cauchy sequences in L to Cauchy sequences in K, and we can conclude that the $x_i := (x_{m,i})_{m\geq 1}$ are elements of $K_\mathfrak{p}$. Therefore, the $b_1, \ldots, b_n$ span $L_\mathfrak{q}$ over $K_\mathfrak{p}$, and we conclude that $[L_\mathfrak{q} : K_\mathfrak{p}] \leq [L : K]$. □

Corollary 3.24. *The completion of a finite extension $K/\mathbb{Q}$ with respect to some prime $\mathfrak{p}$ lying over p, $K_\mathfrak{p}$, is a finite extension of $\mathbb{Q}_p$.*

Now we want to study what happens to completions of Galois extensions. In order to do this we must introduce the decomposition group.

Let L/K be number fields, and let L be Galois over K. For any prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, $\mathrm{Gal}(L/K)$ acts transitively over the primes $\mathfrak{q}$ in $\mathcal{O}_L$ lying over $\mathfrak{p}$, by proposition 2. Set $G = \mathrm{Gal}(L/K)$.

Definition 3.25. *The **decomposition group** of $\mathfrak{q}$ is the stabilizer of $\mathfrak{q}$ in G, denoted by $D_\mathfrak{q} = D_\mathfrak{q}(L/K)$. That is:*

$$D_\mathfrak{q} = \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

By the orbit stabilizer theorem, $[G : D_\mathfrak{q}] = |\{\mathfrak{q} \mid \mathfrak{p}\}| = g_{\mathfrak{q}/\mathfrak{p}}$. Therefore, $|D_\mathfrak{q}| = e_{\mathfrak{q}/\mathfrak{p}}f_{\mathfrak{q}/\mathfrak{p}}$.

Since G acts transitively on the roots of irreducible polynomials, we have that $G(\mathcal{O}_L) = \mathcal{O}_L$. At the same time, $D_\mathfrak{q}$ fixes $\mathfrak{q}$, so every $\sigma \in D_\mathfrak{q}$ induces a field automorphism $\tilde{\sigma}$ of $\mathcal{O}_L/\mathfrak{q}$. Since σ fixes $\mathcal{O}_K$ and $\mathfrak{p}$, $\tilde{\sigma}$ fixes $\mathcal{O}_K/\mathfrak{p}$. To simplify the notation, lets denote $\mathcal{O}_L/\mathfrak{q}$ by $\mathbb{F}_\mathfrak{q}$ and $\mathcal{O}_K/\mathfrak{p}$ by $\mathbb{F}_\mathfrak{p}$. We have a morphism $\pi : D_\mathfrak{q} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$.

This is completely analogous to the morphism φ we defined in the previous section between the Galois group of finite extensions of $\mathbb{Q}_p$ and the Galois group of their residue fields. The only difference is that now we need to consider $D_\mathfrak{q}$ instead of $\mathrm{Gal}(L/K)$ to ensure this morphism is defined.

Proposition 3.26. *The morphism $\pi : D_\mathfrak{q} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ defined above is surjective.*

Proof. The proof is similar to the one for extensions of $\mathbb{Q}_p$. By the primitive element theorem, there will exist $a \in \mathbb{F}_\mathfrak{q}$ such that $\mathbb{F}_\mathfrak{p}(a) = \mathbb{F}_\mathfrak{q}$. Now, for every $\sigma \in G - D_\mathfrak{q}$,

$\sigma^{-1}(\mathfrak{q}) \neq \mathfrak{q}$. So by the chinese remainder theorem we can take some $\alpha \in \mathcal{O}_L$ such that:

$$\alpha \equiv a \pmod{\mathfrak{q}} \text{ and } \alpha \equiv 0 \pmod{\sigma^{-1}(\mathfrak{q})}.$$

Therefore, we can define

$$g(X) = \prod_{\sigma \in G} (X - \sigma(\alpha)) \in K[X].$$

When we take its image modulo $\mathfrak{q}$, we get a polynomial $\tilde{g} \in \mathbb{F}_{\mathfrak{p}}[X]$. If $m = |G - D_{\mathfrak{q}}|$, we can write

$$\tilde{g}(X) = X^m \prod_{\sigma \in D_{\mathfrak{q}}} (X - \tilde{\sigma}(a)).$$

Clearly, the identity in $D_{\mathfrak{q}}$ maps to the identity in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$, so a will be a root of $\tilde{g}$. Therefore all of its conjugates will be of the form $\tilde{\sigma}(a)$, just as we wanted to see. □

Proposition 3.27. *The fixed field $L^{D_{\mathfrak{q}}}$ of $D_{\mathfrak{q}}$ is the smallest subfield F of L such that the prime $\mathfrak{q} \cap F$ doesn't split in L.*

Proof. Since $\mathrm{Gal}(L/L^{D_{\mathfrak{q}}}) = D_{\mathfrak{q}}$ acts transitively on the primes lying over $\mathfrak{q} \cap L^{D_{\mathfrak{q}}}$ and fixes $\mathfrak{q}$, then $\mathfrak{q}$ is the only prime over $\mathfrak{q} \cap L^{D_{\mathfrak{q}}}$.

On the other hand, if $F \subseteq L$ is such that $\mathfrak{q} \cap F$ does not split, since $\mathfrak{q}$ lies over $\mathfrak{q} \cap F$, $\mathrm{Gal}(L/F)$ fixes $\mathfrak{q}$. We must have $\mathrm{Gal}(L/F) \subseteq D_{\mathfrak{q}}$ and hence, $L^{D_{\mathfrak{q}}} \subseteq F$, as we wanted. □

Definition 3.28. *The **inertia group** $I_{\mathfrak{q}} = I_{\mathfrak{q}}(L/K)$ is the kernel of the morphism π. We can write it as:*

$$\{\sigma \in D_{\mathfrak{q}} \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}} \ \forall \alpha \in \mathcal{O}_L\}.$$

By the first isomorphism theorem we have $D_{\mathfrak{q}}/I_{\mathfrak{q}} \cong \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$. Hence, $|I_{\mathfrak{q}}| = e_{\mathfrak{q}/\mathfrak{p}}$.

Proposition 3.29. *Let $L^{I_{\mathfrak{q}}}$ be the fixed field of $I_{\mathfrak{q}}$. Then the idel $\mathfrak{q} \cap L^{I_{\mathfrak{q}}}$ is totally ramified at $\mathfrak{q}$, and the prime $\mathfrak{p}$ is unramified in $L^{I_{\mathfrak{q}}}$.*

Proof. We have that $L/L^{I_{\mathfrak{q}}}$ is Galois, with Galois group I. We can consider the decomposition and inertia groups of $\mathfrak{q}$ over $\mathfrak{p}_I := \mathfrak{q} \cap L^{I_{\mathfrak{q}}}$, $D_{\mathfrak{q}/\mathfrak{p}_I}$ and $I_{\mathfrak{q}/\mathfrak{p}_I}$. We have that

$$D_{\mathfrak{q}/\mathfrak{p}_I} = \{\sigma \in \mathrm{Gal}(L/L^{I_{\mathfrak{q}}}) \mid \sigma(\mathfrak{q}) = \mathfrak{q}\} = I_{\mathfrak{q}}$$

and

$$I_{\mathfrak{q}/\mathfrak{p}_I} = \{\sigma \in \mathrm{Gal}(L/L^{I_{\mathfrak{q}}}) \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}} \ \forall \alpha \in \mathcal{O}_L\} = I_{\mathfrak{q}}.$$

From this we can conclude that $e_{\mathfrak{q}/\mathfrak{p}_I} = |I_{\mathfrak{q}}| = e_{\mathfrak{q}/\mathfrak{p}}$ and $f_{\mathfrak{q}/\mathfrak{p}_I} = 1$. Therefore, $\mathfrak{p}_I$ is totally ramified at $\mathfrak{q}$. By the multiplicativity of the ramification indices, $e_{\mathfrak{p}_I/\mathfrak{p}} = 1$, as we wanted to see. □

Since the completion $K_\mathfrak{p}$ is a finite extension of $\mathbb{Q}_p$, it will be the fraction field of a DVR. Let's denote it by $\mathcal{O}_{K_\mathfrak{p}}$, and its prime ideal by $\hat{\mathfrak{p}}$. We can view $\mathcal{O}_{K_\mathfrak{p}}$ as the completion of $\mathcal{O}_\mathfrak{p}$, and $\hat{\mathfrak{p}}$ as the completion of $\mathfrak{p}\mathcal{O}_\mathfrak{p}$, the prime ideal in $\mathcal{O}_\mathfrak{p}$. Then, the valuation $v_\mathfrak{p}$ defined on K extends with index 1 to the valuation $v_{\hat{\mathfrak{p}}}$ defined on $K_\mathfrak{p}$, and analogously with $v_\mathfrak{q}$. Therefore, $e_{\mathfrak{q}/\mathfrak{p}}(L/K) = e_{\hat{\mathfrak{q}}/\hat{\mathfrak{p}}}(L_\mathfrak{q}/K_\mathfrak{p})$.

We also have that $\mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} \cong \mathcal{O}_{K_\mathfrak{p}}/\hat{\mathfrak{p}}$. The first isomorphism is obvious, let's see the second one. For every Cauchy sequence $(a_n)_{n\geq 1}$ in K there is an $N > 0$ such that $v_\mathfrak{p}(a_n - a_m) > 0$, for every $n, m \geq N$. Therefore, if a_n lives in $\mathcal{O}_\mathfrak{p}$ for n large enough, we will have that $a_n \equiv a_m \pmod{\mathfrak{p}\mathcal{O}_\mathfrak{p}}$, for n and m large enough. We can consider the morphism $\phi : \mathcal{O}_{K_\mathfrak{p}} \to \mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}$ defined by $\phi((a_n)_{n\geq 1}) = a_M \pmod{\mathfrak{p}}$, for a suitable M. Its kernel is the set of Cauchy sequences whose elements are eventually all in $\mathfrak{p}$, which is exactly $\hat{\mathfrak{p}}$. Hence, ϕ induces an isomporphism between $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}$ and $\mathcal{O}_{K_\mathfrak{p}}/\hat{\mathfrak{p}}$.

In the same way, we have an isomorphism of residue fields in L and $L_\mathfrak{q}$. Therefore, the residue field degree will be the same for both extensions:

$$f_{\mathfrak{q}/\mathfrak{p}}(L/K) = f_{\hat{\mathfrak{q}}/\hat{\mathfrak{p}}}(L_\mathfrak{q}/K_\mathfrak{p})$$

We can conclude that $[L_\mathfrak{q} : K_\mathfrak{p}] = e_{\hat{\mathfrak{q}}/\hat{\mathfrak{p}}} f_{\hat{\mathfrak{q}}/\hat{\mathfrak{p}}} = e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}}$.

Now we can state the result concerning completions of Galois extensions of global fields:

Theorem 3.30. *Let $L/K/\mathbb{Q}$ be finite extensions. Let $\mathfrak{q} \mid \mathfrak{p}$ be prime ideals in $\mathcal{O}_L$ and $\mathcal{O}_K$ respectively, lying over a prime $p \in \mathbb{Z}$. If L/K is Galois, so is $L_\mathfrak{q}/K_\mathfrak{p}$ and we have an isomorphism $D_\mathfrak{q}(L/K) \cong \mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p})$ and $I_\mathfrak{q}(L/K) \cong I_{\hat{\mathfrak{q}}}(L_\mathfrak{q}/K_\mathfrak{p}) \subseteq \mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p})$*

Proof. Let $\sigma \in D_\mathfrak{q}(L/K)$. Since it fixes $\mathfrak{q}$, it will also fix $\mathfrak{q}^n$ for every $n \geq 1$. Therefore, if $(a_n)_{n\geq 1}$ is a Cauchy sequence in L, $(\sigma(a_n))_{n\geq 1}$ will also be a Cauchy sequence. Thus, every σ defines an automorphism of $L_\mathfrak{q}$ that fixes $K_\mathfrak{p}$. If σ defines the identity morphism on $L_\mathfrak{q}$, then it will also be the identity on L. Hence, we have that:

$$e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}} = |D_\mathfrak{q}| \leq |\mathrm{Aut}(L_\mathfrak{q}/K_\mathfrak{p})| \leq [L_\mathfrak{q} : K_\mathfrak{p}] = e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}}$$

Therefore we have $|\mathrm{Aut}(L_\mathfrak{q}/K_\mathfrak{p})| = [L_\mathfrak{q} : K_\mathfrak{p}]$, which implies that $L_\mathfrak{q}/K_\mathfrak{p}$ is Galois with $\mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p}) \cong D_\mathfrak{q}(L/K)$.

The image of the inertia group $I_\mathfrak{q}(L/K)$ lies in $I_{\hat{\mathfrak{q}}}(L_\mathfrak{q}/K_\mathfrak{p})$, and they have the same order, so they will be isomorphic.

□

Our objective for the rest of the section is to prove that finite extensions over $\mathbb{Q}_p$ are completions of number fields with respect to some prime lying over p, and that if the local extensions are Galois, then the global extension will also be Galois.

Proposition 3.31. *Let $L/K/\mathbb{Q}$ be finite extensions. Let $\mathfrak{p}$ be a prime in K and consider its natural valuation $v_\mathfrak{p}$. Let w be a valuation on L extending $v_\mathfrak{p}$ with index e. Then there exists a prime $\mathfrak{q}$ in L lying over $\mathfrak{p}$ and with ramification index $e_{\mathfrak{q}/\mathfrak{p}} = e$.*

Proof. Let W be the DVR induced by w in L, and let $\mathfrak{m}$ be its prime ideal. Since w extends $v_\mathfrak{p}$, $\mathcal{O}_\mathfrak{p} \subseteq K$ will be contained in W. Also, the set of elements of $\mathcal{O}_K$ with non-zero valuation by w will be $\mathfrak{p}$. Hence, $\mathfrak{p} = \mathfrak{m} \cap \mathcal{O}_K$. Since discrete valuation rings are Dedekind domains, they are also integrally closed. In particular, W is integrally closed, and since $\mathcal{O}_K \subseteq W$, its integral closure $\mathcal{O}_L$ also lies in W. Let $\mathfrak{q} = \mathfrak{m} \cap \mathcal{O}_L$, a prime ideal in L. Clearly $\mathfrak{q}$ lies above $\mathfrak{p}$.

The ring W will also contain the localization of $\mathcal{O}_L$ with respect to $\mathfrak{q}$, $\mathcal{O}_\mathfrak{q}$, and both rings have the same field of fractions. But there are no intermediate rings between a DVR and its ring of fractions, so $\mathcal{O}_\mathfrak{q} = W$. Therefore, $w = v_\mathfrak{q}$ and $e_{\mathfrak{q}/\mathfrak{p}} = e$, as we wanted to see. □

From this, we trivially get the following corollary.

Corollary 3.32. *Let L/K be finite extensions of number fields. Let $\mathfrak{p}$ be a prime in K. If $|\cdot|$ is an absolute value on L extending $|\cdot|_\mathfrak{p}$, then $|\cdot|$ is the absolute value induced by some prime in L lying over $\mathfrak{p}$.*

Theorem 3.33. *Let $K/\mathbb{Q}$ be a finite extension, and consider $K_\mathfrak{p}$, its completion with respect to some prime $\mathfrak{p}$ in $\mathcal{O}_K$. Every finite extension $\hat{L}$ of $K_\mathfrak{p}$ corresponds to the completion of a finite extension L of K with respect to some prime $\mathfrak{q}$ lying over $\mathfrak{p}$. Whatsmore, we can choose L such that $\hat{L}$ is the compositum of L and $K_\mathfrak{p}$ and $[\hat{L} : K_\mathfrak{p}] = [L : K]$.*

Proof. Since $\hat{L}$ is finite over $K_\mathfrak{p}$, by the primitive element theorem there exists $\alpha \in \hat{L}$ such that $\hat{L} = K_\mathfrak{p}(\alpha)$. Let $f \in K_\mathfrak{p}[X]$ be its irreducible polynomial. Since K is dense in $K_\mathfrak{p}$, we will have that $K[X]$ is dense in $K_\mathfrak{p}[X]$ in the L^1 norm. Therefore, by theorem(Krasner's lemma corollary), there will be a monic irreducible polynomial $g \in K[X]$ and a root β of g such that

$$\hat{L} = K_\mathfrak{p}(\alpha) = K_\mathfrak{p}(\beta).$$

Since g is irreducible in $K_\mathfrak{p}[X]$, it will also be irreducible in $K[X]$. Therefore, setting $L = K(\beta)$, we have $\hat{L} = L \cdot K_\mathfrak{p}$ and $[L : K] = [\hat{L} : K_\mathfrak{p}]$. The absolute value on $\hat{L}$ induces an absolute value on L extending $|\cdot|_\mathfrak{p}$ on K, by restriction. By the previous corollary, $|\cdot|$ will be the absolute value defined by some prime $\mathfrak{q}$ lying over $\mathfrak{p}$. The completion of L with respect to this absolute value contains both L and $K_\mathfrak{p}$, so it also contains $\hat{L}$. Since this field is already complete, the completion of L will be $\hat{L}$, as we wanted to see.

□

Corollary 3.34. *For any finite Galois extension $\hat{L}/\hat{K}$, with $\hat{K}$ finite over $\mathbb{Q}_p$, there corresponds a finite Galois extensions L/K with K finite over $\mathbb{Q}$ and primes $\mathfrak{q} \mid \mathfrak{p}$ in L and K respectively such that $\hat{L}$ is the completion of L with respect to $\mathfrak{q}$ and $\hat{K}$ is the completion of K with respect to $\mathfrak{p}$. Furthermore we have $\mathrm{Gal}(\hat{L}/\hat{K}) \cong \mathrm{Gal}(L/K)$.*

Proof. By the previous theorem, there will exist $K'/\mathbb{Q}$ and an absolute value on K' such that $\hat{K}$ is the completion of K' with respect to this absolute value. Following the proof of the theorem we can write $\hat{L} = \hat{K}(\alpha)$, where α is the root of a polynomial $f \in K'[X]$ irreducible in $\hat{K}$. We also have that $\hat{L}$ is the completion of $L' := K'(\alpha)$ with respect to an extension of the absolute value on K'.

Let L be the normal closure of L' over K', namely the splitting field of f over K'. Since $\hat{L}/\hat{K}$ is Galois and contains both K' and α, it will also contain L. The absolute value on $\hat{L}$ induces an absolute value on L, and clearly $\hat{L}$ will be the completion of L. Now consider the group morphism $\varphi : \mathrm{Gal}(\hat{L}/\hat{K}) \to \mathrm{Gal}(L/K')$ defined by restriction to L. Since $\hat{L} = \hat{K}(\alpha)$, every $\sigma \in \mathrm{Gal}(\hat{L}/\hat{K})$ is defined by the image of α and since $\alpha \in L$, we can conclude that φ is injective.

Set K to be the fixed field of the image of φ. We have $K' \subseteq K \subseteq \hat{K}$, and so the completion of K will be $\hat{K}$. We will have that $\mathrm{Gal}(L/K) = \mathrm{Im}(\varphi) \cong \mathrm{Gal}(\hat{L}/\hat{K})$.

Again, the absolute values on L and K are extensions of the p-adic absolute value on $\mathbb{Q}_p$, so they will be defined by some primes $\mathfrak{q}$ and $\mathfrak{p}$, with $\mathfrak{q} \mid \mathfrak{p}$. □

4 Cyclotomic Fields and Kummer Theory

In this section we will take a look at basic properties of cyclotomic fields, and in particular what happens when the base field is $\mathbb{Q}$ and $\mathbb{Q}_p$. Then we will introduce the concepts of Kummer theory, which we shall use in the proof of the Kronecker-Weber theorem.

Everything in this chapter is standard material for an undergraduate Galois theory course. Any book on Galois theory will cover this material, for example chapter 5 of [Mil17b].

4.1 Cyclotomic Fields

Let K be field, and take $n \geq 1$ prime to the characteristic of K. We will denote by ζ_n a primitive n-th root of unity. We have already seen in chapter 2 that $K(\zeta_n)$ is Galois over K.

Let's recall some basic results on cyclotomic fields.

Lemma 4.1. *i) For every m such that $(m, n) = 1$, ζ_n^m is also a primitive n-th root of unity.*
ii) For any $m \mid n$, $K(\zeta_m) \subseteq K(\zeta_n)$.
iii) $K(\zeta_n) \cdot K(\zeta_n) = K(\zeta_{[m,n]})$.
iv) $K(\zeta_{(m,n)}) \subseteq K(\zeta_n) \cap K(\zeta_n)$, but the equality is not true in general. However, it is true if $K = \mathbb{Q}$.

Proof. i), ii) and iii) are simple to check.

iv) The inclusion is a direct result of ii), since (n, m) divides both n and m. For the reciprocal inclusion, we will give a counterexample:

Take $K = \mathbb{Q}(\sqrt{3})$. Consider $K(\zeta_4) = K(i) = \mathbb{Q}(\sqrt{3}, i)$ and $K(\zeta_3)$. Since $(-1 + \sqrt{-3})/2$ is a primitive 3-rd root of unity, $K(\zeta_3) = \mathbb{Q}(\sqrt{3}, \sqrt{-3}) = \mathbb{Q}(\sqrt{3}, i)$. Therefore, $K(\zeta_4) \cap K(\zeta_3) = K(\zeta_3)$, and it strictly contains $K(\zeta_1) = K$.

Now suppose $K = \mathbb{Q}$. We know that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, for every $n \geq 1$, where φ is the Euler totient function. After some calculations, we see that $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_{(n,m)})$ have the same degree over $\mathbb{Q}$, and since $\mathbb{Q}(\zeta_{(n,m)})$ is contained in the field $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)$, they must be the same. □

We saw in the first chapter that $\mathrm{Gal}\,(K(\zeta_n)/K \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ for every field K, and that for $K = \mathbb{Q}$, we have an isomorphism. Now we will study what happens when $K = \mathbb{Q}_p$.

Lemma 4.2 (p-adic cyclotomic fields)**.** *i) $\mathbb{Q}_p(\zeta_{p^n-1})$ is an unramfied cyclic extension of degree n over $\mathbb{Q}_p$, for every $n \geq 1$.*
ii) $\mathbb{Q}_p(\zeta_{p^r})$ is a totally ramified extension of degree $\varphi(p^r)$ over $\mathbb{Q}_p$. In particular, its Galois group is isomorphic to $(\mathbb{Z}/p^r\mathbb{Z})^*$.
iii) If $p \nmid n$, $\mathbb{Q}_p(\zeta_n)$ is equal to some $\mathbb{Q}_p(\zeta_{p^m-1})$. In particular, it is unramfied and cyclic over $\mathbb{Q}_p$.

Proof. i) We have already seen this in the previous chapter, in Proposition 3.17.

ii) Consider the p^r-th cyclotomic polynomial,

$$\Phi_{p^r}(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = \sum_{i=0}^{p-1} X^{p^{r-1}i}.$$

We will see that the polynomial $\Phi_{p^r}(X+1)$ is p-Eisenstein, and so $\mathbb{Q}_p(\zeta_{p^r}) = \mathbb{Q}_p(\zeta_{p^r}-1)$ is totally ramfied over $\mathbb{Q}_p$.

The constant term is $\Phi_{p^r}(1) = p$. All we need to show now is that the non-leading coefficients are all divisible by p. Let's reduce the polynomial modulo p. Recall that in $\mathbb{F}_p$, $(X^{p^r}-1) = (X-1)^{p^r}$. We have:

$$\frac{X^{p^r}-1}{X^{p^{r-1}}-1} \equiv \frac{(X-1)^{p^r}}{(X-1)^{p^{r-1}}} = (X-1)^{p^{r-1}(p-1)} \pmod{p}.$$

Hence,

$$\Phi_{p^r}(X+1) \equiv X^{p^{r-1}(p-1)} \pmod{p}.$$

Since the degree of $\Phi_{p^r}(X+1)$ is also $p^{r-1}(p-1)$, we can conclude that all the non-leading coefficients are multiples of p. Therefore, it is a p-Eisenstein polynomial and so it is irreducible over $\mathbb{Q}_p$.

We can conclude that $[\mathbb{Q}_p(\zeta_{p^r}) : \mathbb{Q}_p] = \varphi(p^r) = p^{r-1}(p-1)$ and so its Galois group is isomorphic to $(\mathbb{Z}/p^r\mathbb{Z})^*$.

iii) If $p \nmid n$, we want to see that $n \mid p^m - 1$, for some $m \geq 1$. Since $\mathbb{Z}/n\mathbb{Z}$ is finite, we will have $p^a \equiv p^b \pmod{a}$ for some integers $a > b$. Therefore, $n \mid p^{a-b}(p^b-1)$, and since $(n,p) = 1$, $n \mid p^b - 1$ for some $b \geq 1$.

Now, we have that $\mathbb{Q}_p(\zeta_n)$ is a subfield of an unramified extension of $\mathbb{Q}_p$, so it will also be unramified. We saw that there is a bijection between unramified extensions of $\mathbb{Q}_p$ and fields of the form $\mathbb{Q}_p(\zeta_{p^r-1})$, so there exists an m such that $\mathbb{Q}_p(\zeta_n) = \mathbb{Q}_p(\zeta_{p^m-1})$ and we conclude that the extension is cyclic of degree m over $\mathbb{Q}_p$. □

4.2 Kummer Theory

Again, let K be a field and fix $n \geq 1$ prime to the characteristic of K. From now we will suppose that $\zeta_n \in K$.

Consider $a \in K$ and α such that $\alpha^n = a$. Then, $L = K(\alpha)$ contains all the roots of $X^n - a$, since $\zeta_n \in K$. Therefore, $K(\alpha)$ is Galois. We have an injective homomorphism:

$$\begin{aligned} \mathrm{Gal}\,(L/K) &\hookrightarrow \langle \zeta_n \rangle \cong \mathbb{Z}/n\mathbb{Z} \\ \sigma &\mapsto \frac{\sigma(\alpha)}{\alpha} \end{aligned}$$

Hence, L/K is cyclic of degree d, for some $d \mid n$. Moreover, $\alpha^d \in K$. Taking σ a generator of $\mathrm{Gal}(L/K)$, we have that $\sigma(\alpha^d) = \sigma(\alpha)^d = (\zeta_d\alpha)^d = \alpha^d$, so $\alpha^d \in K^*$. Kummer's key observation is that the converse also holds:

Proposition 4.3. *Let L/K be cyclic of degree n, with $\zeta_n \in K$. Then there exists an $a \in K^*$ such that $L = K(\sqrt[n]{a})$.*

Proof. Let σ be a generator of $\mathrm{Gal}(L/K)$. Since $\mathrm{N}_{L/K}(\zeta_n) = \zeta_n^n = 1$, we can apply Hilbert's Theorem 90 (lemma 4.4 below), and obtain an element $\alpha \in L$ such that $\sigma(\alpha) = \zeta_n \alpha$. Since $\mathrm{Id}, \sigma, \ldots, \sigma^{n-1}$ are all distinct automorphisms, $\sigma^i(\alpha) = \zeta_n^i \alpha$ will also be different elements of L. This implies that $[K(\alpha) : K] \geq n$, and since L/K already has degree n, $L = K(\alpha)$.

Moreover, we have that

$$\sigma(\alpha^n) = \sigma(\alpha)^n = \zeta_n^n \alpha^n = \alpha^n$$

Therefore, α^n must be an element of K. In other words, α is a root of the polynomial $X^n - a$, where $a = \alpha^n \in K$, as we wanted to see. □

Lemma 4.4 (Hilbert's Theorem 90)**.** *Let L/K be a cyclic extension, and let σ be a generator of the Galois group. For every $u \in L$ with $\mathrm{N}_{L/K}(u) = 1$ there exists $\alpha \in L^*$ such that $\sigma(\alpha) = u\alpha$.*

Let $\overline{K}$ be an algebraic closure of K. The ***Kummer Pairing*** is the bilinear map:

$$\begin{aligned} \langle \cdot, \cdot \rangle : \mathrm{Gal}(\overline{K}/K) \times K^*/K^{*n} &\to \langle \zeta_n \rangle \\ (\sigma, \overline{a}) &\mapsto \langle \sigma, \overline{a} \rangle = \sigma(\alpha)/\alpha \end{aligned}$$

where $\overline{a}$ is the class of $a \in K^*$ modulo K^{*n} and α is an n-th root of a in $\overline{K}$. For any $c \in K^{*n}$, $\langle \sigma, \overline{c} \rangle = 1$, and so the pairing doesn't depend on the choice of representative of $\overline{a}$. Let β be an n-th root of a different from α. Then α/β is an n-th root of unity and therefore will be fixed by σ, since all n-th roots of unity live in K. Therefore, we have that $\sigma(\beta)/\beta = \sigma(\beta)/\beta \cdot \sigma(\alpha/\beta)/(\alpha/\beta) = \sigma(\alpha)/\alpha$. So the pairing doesn't depend on the choice of α. In conclusion, it is well defined.

Definition 4.5. *Let K be a field with $\zeta_n \in K$. An extension L/K is called an **n-Kummer extension of K** if L/K is Galois with abelian Galois group of exponent n, i.e. such that every $\sigma \in \mathrm{Gal}(L/K)$ has order dividing n.*

Theorem 4.6. *There is a bijection between finite subgroups of K^*/K^{*n} and finite n-Kummer extensions of K, given by the mapping:*

$$A \mapsto K(A^{1/n}).$$

Proof. Let A be a finite subgroup of K^*/K^{*n}. By the structure theorem of finitely generated groups, there exists $a_1, \ldots, a_r \in K^*$ such that

$$A = \langle \overline{a_1} \rangle \times \cdots \times \langle \overline{a_r} \rangle.$$

Let n_i be the order of $\overline{a_i}$ in K^*/K^{*n}, $n_i \mid n$. Consider α_i such that $\alpha_i^n = a_i$. If $s \in \mathbb{Z}$ is such that $\alpha_i^s = c \in K^*$, we will have

$$a_i = \alpha_i^n = c^{n/s} \implies a_i^s = c^n.$$

Therefore, $n_i \mid s$. In other words, n_i is the minimum integer such that $\alpha_i^{n_i} \in K^*$. We can conclude that $L_i = K(\sqrt[n]{a_i})$ is cyclic of degree $[L_i : K] = n_i$.

The fields L_i will be linearly disjoint, because the a_i are independent generators of A. Hence, $L = L_1 \cdots L_r = K(A^{1/n})$ has Galois group isomorphic to A, and so L/K is an n-Kummer extension.

Let's show that for any two subgroups $A, B \subseteq K^*/K^{*n}$, $K(A^{1/n}) = K(B^{1/n})$ implies $A = B$. In other words, we have an injection of our set of groups into the set of n-Kummer extensions of K. We only need to show that $K(A^{1/n}) \subseteq K(B^{1/n})$ implies $A \subseteq B$, and the result will follow by symmetry.

Let $a \in K^*$ such that $\overline{a} \in A$. Then, $K(\sqrt[n]{a}) \subseteq K(B^{1/n})$. Let $C = \langle B, \overline{a} \rangle$, a finite subgroup of K^*/K^{*n}. We will have that $K(B^{1/n}) = K(C^{1/n})$. We have just seen that $|\operatorname{Gal}(K(D^{1/n})/K)| = |D|$, for any subgroup $D \subseteq K^*/K^{*n}$, so we must have $|B| = |C|$. Hence, $B = C$ and in particular $\overline{a} \in B$, as we wanted to see.

Conversely, given a finite n-Kummer extension L/K, by the structure theorem of finite abelian groups, we can write $\operatorname{Gal}(L/K)$ as the product of $r \geq 1$ finite cyclic subgroups. Let $L_1, \ldots, L_r$, the fixed fields of these cyclic subgroups. Each L_i will be cyclic over K, and by Lemma 5.4, $L_i = K(\sqrt[n_i]{a_i})$, for some $a_i \in K^*$ and $n_i \mid n$. Therefore, defining $A := \langle \overline{a_1} \rangle \times \cdots \times \langle \overline{a_r} \rangle$, we have a subgroup of K^*/K^{*n} such that $K(A^{1/n}) = L$.

□

When $\zeta_n \in K$, Kummer theory is a very useful tool to study the abelian extensions of K. However, if we are not in this situation, things can be quite complicated. The following lemma will help us handle the case when n is a prime and not necessarily $\zeta_n \in K$.

Lemma 4.7. *Let n be prime, F a field of characteristic prime to n and let $L = K(\sqrt[n]{a})$, for some $a \in K^*$. Define the homomorphism $\omega : \operatorname{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^*$ by $\zeta_n^{\omega(\sigma)} = \sigma(\zeta_n)$. If L/F is abelian, then $\sigma(a)/a^{\omega(\sigma)} \in K^{*n}$, for all $\sigma \in \operatorname{Gal}(L/K)$.*

Proof. Let $G = \operatorname{Gal}(L/F)$, $H = \operatorname{Gal}(L/K) \subseteq G$, and let $A = \langle \overline{a} \rangle \subseteq K^*/K^{*n}$. Since $L = K(A^{1/n})$, we have a bilinear pairing induced by the Kummer pairing: $H \times A \to \langle \zeta_n \rangle$. If $\overline{b} \in A$ is such that $\langle h, \overline{b} \rangle = 1$ for every $h \in H$, then $b \in K^{*n}$. Suppose not, then $K(\sqrt[n]{b})/K$ is a non-trivial extension and so there will be some automorphism of $K(\sqrt[n]{b})$ that doesn't fix $\sqrt[n]{b}$. Extending this automorphism to L, we'd have a $\sigma \in H$ such that $\langle h, \overline{b} \rangle \neq 1$, a contradiction. Therefore, we have that $b \in K^{*n}$, as we wanted.

$\operatorname{Gal}(K/F)$ acts on A, in a natural way. It is well defined because it sends n-th powers to n-th powers. Let $\alpha \in L$ be such that $\alpha^n = a$. Then for every $\sigma \in \operatorname{Gal}(K/F)$, if $\tilde{\sigma} \in \operatorname{Gal}(L/F)$ is an extension of σ, we have that $\tilde{\sigma}(\alpha)^n = \sigma(a)$.

It also acts on H by conjugation: extend $\sigma \in \operatorname{Gal}(K/F)$ to a $\tilde{\sigma} \in \operatorname{Gal}(L/F)$ and define $h^\sigma = \tilde{\sigma} h \tilde{\sigma}^{-1}$. It is well defined, since for any two extensions $\tilde{\sigma}$ and $\tilde{\mu}$ of σ, there exists $\tau \in \operatorname{Gal}(L/K)$ such that $\tilde{\sigma} = \tau\tilde{\mu}$. Hence, $h^{\tilde{\sigma}} = h^{\tau\tilde{\mu}} = (h^\tau)^{\tilde{\mu}} = h^{\tilde{\mu}}$, since $\operatorname{Gal}(L/K)$ is abelian and so $h^\tau = h$.

These actions commute with the action of $\operatorname{Gal}(K/F)$ on ζ_n:

$$\sigma(\langle h, a\rangle) = \frac{\tilde{\sigma}(h(a^{1/n}))}{\tilde{\sigma}(a^{1/n})} = \frac{h^{\sigma}(\tilde{\sigma}(a^{1/n}))}{\tilde{\sigma}(a^{1/n})} = \frac{h^{\sigma}(\sigma(a)^{1/n})}{\sigma(a)^{1/n}} = \langle h^{\sigma}, \sigma(a)\rangle$$

Now, in our case, $\mathrm{Gal}(L/F)$ is abelian, and so the action of $\mathrm{Gal}(K/F)$ on $\mathrm{Gal}(L/K)$ by conjugation is trivial. Hence, we have:

$$\langle h, a^{\omega(\sigma)}\rangle = \langle h, a\rangle^{\omega(\sigma)} = \sigma(\langle h, a\rangle) = \langle h, \sigma(a)\rangle$$

Therefore, $\langle h, \sigma(a)/a^{\omega(\sigma)}\rangle = 1$ for every $h \in H$, and as we saw earlier, this means that $\sigma(a)/a^{\omega(\sigma)} \in K^{*n}$, just as we wanted to prove $\square$

5 Kronecker-Weber Theorem

This chapter is entirely dedicated to the proof of the Kronecker-Weber theorem. We have developed all the theory and results we need in the previous chapters, and we will use them extensively in our proof. We begin by showing that the local-global principle works, and then we prove the local case. We follow Washington's proof in chapter 14 of [Was97], as well as chapter 20 of [Sut17].

5.1 Local-Global Principle

Let's state the global and local versions of the Kronecker-Weber theorem.

Theorem 5.1 (Global Kronecker-Weber Theorem)**.** *Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta_m)$, for some $m \geq 1$.*

Theorem 5.2 (Local Kronecker-Weber Theorem)**.** *Every finite abelian extension of $\mathbb{Q}_p$ is contained in a cyclotomic extension $\mathbb{Q}_p(\zeta_m)$, for some $m \geq 1$.*

Theorem 5.3. *The Global K-W Theorem holds if and only if the Local K-W Theorem holds for every prime p.*

Proof. Suppose the Global K-W theorem holds, and suppose $\hat{K}/\mathbb{Q}_p$ is a finite abelian extension. By corollary 3.34, there corresponds a global Galois extension $K/\mathbb{Q}$ such that $\hat{K}$ is the completion of K with respect to the $\mathfrak{p}$-adic absolute value, for some prime $\mathfrak{p} \mid p$. We also have that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(\hat{K}/\mathbb{Q}_p)$, so $K/\mathbb{Q}$ is a finite abelian extension. By the global K-W theorem, there exists $m \geq 1$ such that $K \subseteq \mathbb{Q}(\zeta_m)$. Let $\hat{L}$ be the completion of $L = \mathbb{Q}(\zeta_m)$ at a prime $\mathfrak{q} \in \mathcal{O}_L$ over $\mathfrak{p}$, so $\hat{K} \subseteq \hat{L}$. Since $\mathfrak{q}$ is a prime over p, $\hat{L}$ contains the field $\mathbb{Q}_p(\zeta_m)$, which already is complete. Hence, $\hat{L} = \mathbb{Q}_p(\zeta_m)$. We can conclude that $K \subseteq \mathbb{Q}_p(\zeta_m)$, as we wanted to see.

Now suppose that the local K-W holds for every prime p, and let $K/\mathbb{Q}$ be a finite abelian extension. We know there are only finitely many primes that ramify in K, let's denote them by $p_1, \ldots, p_s$. Pick primes $\mathfrak{p}_i$ in $\mathcal{O}_K$ such that $\mathfrak{p}_i \mid p_i$. By theorem 3.30, each $\mathrm{Gal}(K_{\mathfrak{p}_i}/\mathbb{Q}_p)$ is isomorphic to a subgroup of $\mathrm{Gal}(K/\mathbb{Q})$, and hence the $K_{\mathfrak{p}_i}$ are finite abelian extensions of $\mathbb{Q}_{p_i}$. We are assuming that the local Kronecker-Weber theorem holds for every prime p_i, so there exist integers $m_i \geq 1$ such that $K_{\mathfrak{p}_i} \subseteq \mathbb{Q}_{p_i}(\zeta_{m_i})$, for every i. Let e_i be the maximum power of p_i diving m_i, i.e. $e_i = v_{p_i}(m_i)$, and consider $m = \prod_{i=1}^{s} p_i^{e_i}$. We claim that $K(\zeta_m) = \mathbb{Q}(\zeta_m)$, and in particular $K \subseteq \mathbb{Q}(\zeta_m)$.

Let $L = K(\zeta_m) = K \cdot \mathbb{Q}(\zeta_m)$. Since it is a cyclotomic extension, it will be Galois over K, and hence also over $\mathbb{Q}$. We will also have that $\mathrm{Gal}(L/\mathbb{Q})$ is a subgroup of $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, and so it will be finite abelian over $\mathbb{Q}$.

Let $\mathfrak{q}_i$ be a prime in $\mathcal{O}_L$ lying over $\mathfrak{p}_i$, and consider the completion $L_{\mathfrak{q}_i}/\mathbb{Q}_{p_i}$. Let F_i be the maximal unramified extension of $\mathbb{Q}_{p_i}$ in $L_{\mathfrak{q}_i}$. We have that $L_{\mathfrak{q}_i}/F$ is totally ramified and its Galois group is isomorphic to the inertia group $I_i := I_{\mathfrak{q}_i} \subseteq \mathrm{Gal}(L/\mathbb{Q})$, by theorem 3.30. We know that F_i contains all roots of unity ζ_n with $n \mid m$ and

$(n, p_i) = 1$. Therefore, $L_{\mathfrak{q}_i} = F_i(\zeta_m) = F_i(\zeta_{p_i^{e_i}})$. Since $\mathbb{Q}_{p_i}(\zeta_{p_i^{e_i}})$ is totally ramified over $\mathbb{Q}_{p_i}$ and F_i is unramified over $\mathbb{Q}_{p_i}$, their intersection must be $\mathbb{Q}_{p_i}$. Hence,

$$I_i \cong \mathrm{Gal}(L_{\mathfrak{q}_i}/F_i) \cong \mathrm{Gal}(\mathbb{Q}_{p_i}(\zeta_{p_i^{e_i}}))/\mathbb{Q}_{p_i}) \cong (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*.$$

Now let I be the subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ generated by the inertia groups I_i. Since $\mathrm{Gal}(L/\mathbb{Q})$ is abelian, we have that

$$|I| \leq \prod_{i=1}^{s} |I_i| = \prod_{i=1}^{s} \varphi(p_i^{e_i})$$

The Euler totient function φ is multiplicative, i.e. $\varphi(nm) = \varphi(n)\varphi(m)$ if $(n, m) = 1$. Therefore,

$$|I| \leq \varphi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$$

Now let p be a prime in $\mathbb{Z}$ that is unramified in K. Let $\mathfrak{p}$ and $\mathfrak{q}$ be primes in K and L, satisfying $\mathfrak{q} \mid \mathfrak{p} \mid p$, and let $L_\mathfrak{q}$ and $K_\mathfrak{p}$ be the completions of L and K with respect to these primes. We will have that $L_\mathfrak{q} = K_\mathfrak{p}(\zeta_m)$. Since $p \nmid m$, $L_\mathfrak{q}$ is unramified over $K_\mathfrak{p}$. Hence, $I_\mathfrak{q}(L/K) \cong I_{\hat{\mathfrak{q}}}(L_\mathfrak{q}/K_\mathfrak{p}) = (1)$ and so $\mathfrak{p}$ is unramified in L. Since p is also unramified in K, and $\mathfrak{q} \mid \mathfrak{p} \mid p$, we can conclude that p will be unramified in L.

Therefore, every prime that ramifies in L will also ramify in K. Since $I_i \subseteq I$, the primes p_i will be unramified in L^I. Hence, no primes of $\mathbb{Q}$ ramify in L^I. By the following lemma, L will be a trivial extension. You can find a proof of this lemma in [Sut17], in proposition 14.21.

Lemma 5.4. *If $L/\mathbb{Q}$ is a finite extension such that no prime of $\mathbb{Q}$ ramifies in L, then $L = \mathbb{Q}$.*

Therefore, $I \cong \mathrm{Gal}(L/K^I) = \mathrm{Gal}(L/\mathbb{Q})$. Since $L/\mathbb{Q}(\zeta_m)$, and $[L : \mathbb{Q}] = \varphi(m)$, we can conclude that $\mathbb{Q}(\zeta_m) = L$, as we wanted to see. □

5.2 Local Case

If L/K is an abelian Galois extension with Galois group $\mathrm{Gal}(L/K) = H_1 \times H_2$, we can define the fixed fields $L_1 = L^{H_1}$ and L^{H_2}. We then have that $L = L_1 \cdot L_2$, $L_1 \cap L_2 = K$ and $\mathrm{Gal}(L_i/K) \cong H_i$. It then follows from the structure theorem for finite abelian groups that we can decompose any finite abelian extension $K/\mathbb{Q}_p$ into the compositum of cyclic extensions of prime power order: $K = K_1 \cdots K_n$. Thus, if we show that every cyclic extension of prime power degree over $\mathbb{Q}_p$ is cyclotomic, then we would have that each K_i is contained in $\mathbb{Q}_p(\zeta_{m_i})$, for some m_i, and taking $m = m_1 \cdots m_n$ we would have $K \subseteq \mathbb{Q}_p(\zeta_m)$.

In order to prove the local Kronecker-Weber theorem, we will consider cyclic l-extensions $K/\mathbb{Q}_p$, where l is a prime number. We will separate the proof in three cases: $l \neq p$, $l = p \neq 2$ and $l = p = 2$. For the first case we will use a combination of results of finite extensions of $\mathbb{Q}_p$ from chapter 3. For the other two cases, however, things are a little bit more complex, and we will need to use Kummer theory.

Theorem 5.5. *Let $K/\mathbb{Q}_p$ be a cyclic extension of degree l^r for some prime $l \neq p$. Then there exists an $m \geq 1$ such that $K \subseteq \mathbb{Q}_p(\zeta_m)$*

Proof. Let F be the maximal unramified subextension of K. We have seen in the previous chapter that $F = \mathbb{Q}_p(\zeta_n)$ for some n. K/F will be totally ramified, and since $p \neq l$, it will also be tamely ramified. By proposition 3.16, $K = F(\pi^{1/e})$, for a uniformizer π of F. Since the extension $F/\mathbb{Q}_p$ is unramified, $|\pi/(-p)| = 1$ and we can write $\pi = -pu$, for some unit $u \in \mathcal{O}_K^*$. Now we have that $K = F((-pu)^{1/e}) \subseteq F((-p)^{1/e}) \cdot F(u^{1/e})$. We will show that both fields are cyclotomic.

Consider the polynomial $X^e - u$, whose roots are $u^{1/e}, \zeta_e u^{1/e}, \ldots, \zeta_e^{e-1} u^{1/e}$. The discriminant of $f(X) = \prod_{i=1}^n (X - \alpha_i)$ is equal to $(-1)^{n(n-1)/2} \prod f'(\alpha_i)$. So we will have that the discriminant of $X^e - u$ is

$$(-1)^{e(e-1)/2} \prod_{i=0}^{e-1} e(\zeta_e^i u^{1/e})^{e-1}.$$

Calculating, we get that this is equal to

$$(-1)^m e^e u^{e-1} \zeta_e^{e(e-1)/2} = e^e u^{e-1},$$

for some m. Since $p \nmid e$ and u is a unit, p will not divide the discriminant of $X^e - u$. Therefore, p won't divide the discriminant of the extension and we will have that p does not ramify in $F(u^{1/e})$. So $F(u^{1/e})/F$ is unramified, and $F(u^{1/e})$ will also be unramified over $\mathbb{Q}_p$. Therefore, $F(u^{1/e}) = \mathbb{Q}_p(\zeta_k)$ for some k, and so it is a cyclic Galois extension over $\mathbb{Q}_p$.

This implies that $K(u^{1/e}) = K \cdot \mathbb{Q}_p(u^{1/e})$ is a compositum of abelian extensions and therefore abelian itself. In turn, this implies that its subextension $\mathbb{Q}_p((-p)^{1/e})$ will also be Galois over $\mathbb{Q}_p$. Hence, all the roots of the Eisenstein polynomial $X^e + p$ live in $\mathbb{Q}_p((-p)^{1/e})$. The roots will be of the form $\zeta_e^i(-p)^{1/e}$, where $0 \leq i \leq e$, so taking ratios we get that ζ_e lives in $\mathbb{Q}_p((-p)^{1/e})$. Now, we would have that $\mathbb{Q}_p(\zeta_e)$ is a totally ramified extension of $\mathbb{Q}_p$, but since $p \nmid e$, $\mathbb{Q}_p(\zeta_e)$ is unramified over $\mathbb{Q}_p$. There is no other choice but $\mathbb{Q}_p(\zeta_e) = \mathbb{Q}_p$, and so $e \mid p-1$ if $p \neq 2$. If $p = 2$, since $p \nmid e$, we have that $e = 1$. In both cases, this means that $\mathbb{Q}_p((-p)^{1/e}) \subseteq \mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$, by lemma 3.12. Hence, $F((-p)^{1/e}) = F \cdot \mathbb{Q}_p((-p)^{1/e}) \subseteq \mathbb{Q}_p(\zeta_{np})$.

Combining the results, we have that for $m = npk$

$$K \subseteq F(u^{1/e}) \cdot F((-p)^{1/e}) \subseteq \mathbb{Q}_p(\zeta_m)$$

This finishes the proof.

□

Theorem 5.6. *Let $p \neq 2$ be a prime, and let $K/\mathbb{Q}_p$ be a cyclic extension of degree p^r, $r \geq 1$. Then there exists an $m \geq 1$ such that $K \subseteq \mathbb{Q}_p(\zeta_m)$*

Proof. We know that $\mathbb{Q}_p(\zeta_{p^{r+1}})$ is an abelian extension of order $\varphi(p^{r+1}) = p^r(p-1)$ and Galois group isomorphic to $(\mathbb{Z}/p^{r+1}\mathbb{Z})^*$, and hence cyclic. The fixed field of

the $p-1$ index subgroup will be cyclic of degree p^r over $\mathbb{Q}_p$, and it is obviously contained in a cyclotomic extension. We also saw that $\mathbb{Q}_p(\zeta_{p^{p^r}-1})$ is a cyclic extension of degree p^r. We will show that K will be contained in their compositum, $\mathbb{Q}_p(\zeta_m)$, with $m = p^{r+1}(p^{p^r}-1)$.

For the sake of contradiction, suppose that K isn't contained in $\mathbb{Q}_p(\zeta_m)$. Therefore, $K(\zeta_m)$ is a non-trivial extension of $\mathbb{Q}_p(\zeta_m)$, and since $K/\mathbb{Q}$ is cyclic of degree p^r, $\mathrm{Gal}(K(\zeta_m)/\mathbb{Q}_p(\zeta_m)) \cong \mathbb{Z}/p^s\mathbb{Z}$, for some $1 < s \leq r$. Now, recall that $\mathbb{Q}_p(\zeta_{p^{r+1}})$ is totally ramified over $\mathbb{Q}_p$ and $\mathbb{Q}_p(\zeta_{p^{p^r}-1})$ is unramified over $\mathbb{Q}_p$, so their intersection is $\mathbb{Q}_p$ and

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) \cong \mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}.$$

We have:

$$\mathrm{Gal}(K(\zeta_m)/\mathbb{Q}_p) \hookrightarrow (\mathbb{Z}/p^r\mathbb{Z})^3 \times \mathbb{Z}/(p-1)\mathbb{Z}$$

Since $\mathrm{Gal}(K(\zeta_m)/\mathbb{Q}_p)$ has a subgroup isomorphic to $\mathbb{Z}/p^s\mathbb{Z}$ with quotient isomorphic to $(\mathbb{Z}/p^r\mathbb{Z})^2 \times \mathbb{Z}/(p-1)\mathbb{Z}$, we can conclude that:

$$\mathrm{Gal}(K(\zeta_m)/\mathbb{Q}_p) \cong \mathbb{Z}/p^s \times (\mathbb{Z}/p^r\mathbb{Z})^2 \times \mathbb{Z}/(p-1)\mathbb{Z}$$

In particular, it will have a subextension $N \subseteq K(\zeta_m)$ with Galois group over $\mathbb{Q}_p$ isomorphic to $(\mathbb{Z}/p\mathbb{Z})^3$. However, we will show that no such extension exists.

Lemma 5.7. *For $p \neq 2$ there are no extension $N/\mathbb{Q}_p$ with Galois group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^3$.*

Proof. Since $[\mathbb{Q}_p(\zeta_p) : \mathbb{Q}_p] = p-1$, $\mathbb{Q}_p(\zeta_p)$ and N will be linearly disjoint and so

$$G := \mathrm{Gal}(N(\zeta_p)/\mathbb{Q}_p(\zeta_p)) \cong (\mathbb{Z}/p\mathbb{Z})^3.$$

We have that $N(\zeta_p)$ is a p-Kummer extension of $\mathbb{Q}_p(\zeta_p)$, so by theorem 4.6, there exists a subgroup $B \subseteq \mathbb{Q}_p(\zeta_p)^*/\mathbb{Q}_p(\zeta_p)^{*p}$ such that

$$N(\zeta_p) = \mathbb{Q}_p(\zeta_p, B^{1/p}), \text{ and } B \cong (\mathbb{Z}/p\mathbb{Z})^3.$$

Let $\overline{a} \in B$ and set $L = \mathbb{Q}_p(\zeta_p, \sqrt[p]{a}) \subseteq N(\zeta_p)$.

Since $\mathrm{Gal}(N(\zeta_p)/\mathbb{Q}_p)$ is a subgroup of $\mathrm{Gal}(N/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)$, it will be abelian. Now, $\mathrm{Gal}(L/\mathbb{Q}_p)$ is a quotient of $\mathrm{Gal}(N(\zeta_p)/\mathbb{Q}_p)$, so it will also be abelian. Therefore, we can apply lemma 4.7 to L and we get:

$$\sigma(a)/a^{\omega(\sigma)} \in \mathbb{Q}_p(\zeta_p)^{*p}$$

for all $\sigma \in G$, where $\omega : G \to (\mathbb{Z}/p\mathbb{Z})^*$ is the morphism (in fact isomorphism) defined by $\sigma(\zeta_p) = \zeta_p^{\omega(\sigma)}$.

Take $\pi = \zeta_p - 1$ as a uniformizer of $\mathbb{Q}_p(\zeta_p)$, which we already know is a totally ramified extension of $\mathbb{Q}_p$ with residue field isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Consider the subgroup of the ring of integers of $\mathbb{Q}_p(\zeta_p)$, $U_1 := \{u \mid u \equiv 1 \pmod{\pi}\}$. We will show that for each $\overline{a} \in B$, we will have a representative $a \in U_1$. Hence, we can consider $B \subseteq U_1/U_1^p$.

Since $\sigma(a) = a^{\omega(\sigma)}\alpha^p$, for some $\alpha \in \mathbb{Q}_p(\zeta_p)^*$, we have:

$$v_\pi(a) = v_\pi(\sigma(a)) = v_\pi(a^{\omega(\sigma)}) + pv_\pi(\alpha) \equiv \omega(\sigma)v_\pi(a) \pmod{p},$$

where v_π is the valuation relative to π in $\mathbb{Q}_p(\zeta_p)$. Then we have

$$(1 - \omega(\sigma))v_\pi(a) \equiv 0 \pmod{p},\ \forall \sigma \in G,$$

and since ω is an isomorphism, $\omega(\sigma)$ will range over all the elements of $(\mathbb{Z}/p\mathbb{Z})^*$. This means that $v_\pi(a) \equiv 0 \pmod{p}$. Since multiplying a by a p-th power doesn't change $\overline{a}$, we can consider as a representative $a\pi^{-v_\pi(a)}$, and denote it again by a. Observe that now $v_\pi(a) = 0$ and $a \not\equiv 0 \pmod{\pi}$.

Recall that the powers of ζ_{p-1} form a complete set of representatives of the residue field of $\mathbb{Q}_p$. Since the residue field hasn't grown in our extension (it is totally ramified), they will still be a complete set of representatives of the residue field of $\mathbb{Q}_p(\zeta_p)$. Observe too that $\zeta_{p-1}^p = \zeta_{p-1}$, so multiplying a by any of its powers doesn't change our class modulo $\mathbb{Q}_p(\zeta_p)^{*p}$. Choosing a suitable power, we will have $\zeta_{p-1}^b a \equiv 1 \pmod{\pi}$. Therefore, we can choose a representative of $\overline{a}$ that lives in U_1.

Now, taking any element $u \in U_1$, we can write it as a power series in π with integer coefficients in $[0, p-1]$ (since these form a complete set of representatives of the classes of the residue field) and constant coefficient 1. In particular, let $u = 1 + b\pi + O(\pi^2)$, with $b \in \mathbb{Z}$. Here the expression $O(\pi^k)$ denotes a power series in π divisible by π^k, for any $k \geq 0$.

Since $\zeta_p = 1 + \pi$, we will have $\zeta_p^b = 1 + b\pi + O(\pi^2)$ for every $b \in [0, p-1]$. Define $u_1 := \zeta_p^{-b} a = 1 + O(\pi^2)$. Hence, every element $u \in U_1$ can be written as $u = \zeta_p^b u_1$, for some $b \in \mathbb{Z}$ and $u_1 \equiv 1 \pmod{\pi^2}$. We know that $p = \pi^{p-1}$, so we will have $p\pi^2 \equiv 0 \pmod{\pi^{p+1}}$. Since every interior term of the binomial expansion of $(1 + \pi^2\alpha)^p$ other than 1 is divisible by $p\pi^2$, we have that $u_1^p \equiv 1 \pmod{\pi^{p+1}}$. Therefore, $u^p = u_1^p \equiv 1 \pmod{\pi^{p+1}}$. So $U_1^p \subseteq \{u \mid u \equiv 1 \pmod{\pi^{p+1}}\}$.

Lemma 5.8. $U^p = \{u \mid u \equiv 1 \pmod{\pi^{p+1}}\}$

Proof. We have just seen one inclusion, now let's see the converse one. For this we will make use of the p-adic logarithm and exponential. Since finite extensions of $\mathbb{Q}_p$ are complete non-archimedean valued fields, we can apply the results of p-adic analysis we studied in section 2.4. In particular, log and exp will have the same radius of convergence, since the proof for $\mathbb{Q}_p$ works in general for any finite extension.

Define the function $f(X) = \exp(\frac{1}{p}\log(x))$. Observe that, supposing everything is well defined, $f(x)^p = \exp(\frac{p}{p}\log(x)) = \exp(\log(x)) = x$. So if we prove that for every v satisfying $v \equiv 1 \pmod{\pi^{p+1}}$, $f(v)$ is well defined and $f(v) \in U_1$, then $v = f(v)^p \in U_1^p$, as we want to show.

We know that $\log(1+x)$ is well defined for any x with $|x| < 1$. Since $u_1 = 1+\pi^{p+1}\alpha$, for some α with $|\alpha| \leq 1$, $\log(u_1)$ is well defined. By the definition of log as a power series,

$$\log(u_1) = \sum_{n \geq 1} (-1)^{n+1} \frac{(\pi^{p+1}\alpha)^n}{n}.$$

Dividing by p is the same as dividing by $\pi^{p-1}w$, where $\pi \nmid w$, so

$$\frac{1}{p}\log(u_1) = \pi^{p+1-(p-1)}\alpha + O(\pi^{2(p+1)-(p-1)}) = \pi^2\alpha + O(\pi^3).$$

We can write $\pi^2\alpha + O(\pi^{p+3}) = \pi^2\beta$, for some $|\beta| \leq 1$. Now, we have that

$$|\pi^2\beta| \leq |\pi|^2 = |p|^{2/(p-1)} < |p|^{1/(p-1)}.$$

The function $\exp(x)$ is defined for $|x| < |p|^{1/(p-1)}$, so $f(u_1)$ is well defined for every $u_1 \equiv 1 \pmod{\pi^{p+1}}$.

Now, by the definition of $\exp(x)$ we see that

$$f(u_1) = 1 + \sum_{n\geq 1} \frac{(\pi^2\beta)^n}{n!}$$

Since $v_p(n!) = \frac{n-S_p(n)}{p-1}$, we have that $v_\pi(n!) = n - S_p(n)$, where $S_p(n)$ is the sum of the digits of n in base p, and so $S_p(n) \geq 0$. With this, we can see that for $n \geq 1$

$$v_\pi(\pi^{2n}\beta^n/(n!)) \geq 2n - v_\pi(n!) = 2n - n + S_p(n) \geq n$$

In conclusion, $f(u_1) \equiv 1 \pmod{\pi}$ and so $f(u_1) \in U$, as we wanted to see.

□

Let's go back to our discussion of $\mathbb{Q}_p(\zeta_p)^*/\mathbb{Q}_p(\zeta_p)^{*p}$. For every $\sigma \in G$ we have

$$\frac{\sigma(\pi)}{\pi} = \frac{\zeta_p^{\omega(\sigma)} - 1}{\zeta_p - 1} = \zeta_p^{\omega(\sigma)-1} + \cdots + \zeta_p + 1 \equiv \omega(\sigma) \pmod{\pi}$$

where we are considering $\omega(\sigma)$ as an integer in $[0, p-1]$. Therefore we must have that $\sigma(\pi)^e/\pi^e \equiv \omega(\sigma)^e \pmod{\pi}$, which in turn implies $\sigma(\pi)^e = \pi^e\omega(\sigma)^e + O(\pi^{e+1})$.

Let's write $a = \zeta_p^b(1 + c\pi^e + O(\pi^{e+1}))$, for some $c \in \mathbb{Z}$ and $e \geq 2$. We will have that:

$$\sigma(a) = \zeta_p^{\omega(\sigma)b}(1 + c\omega(\sigma)^e\pi^e + O(\pi^{e+1})).$$

At the same time, we have:

$$a^{\omega(\sigma)} = \zeta_p^{\omega(\sigma)b}(1 + c\omega(\sigma)\pi^e + O(\pi^{e+1})).$$

We have already seen that $\sigma(a)/a^{\omega(\sigma)} \in U_1^p$, so by the previous lemma we get $\sigma(a) = a^{\omega(\sigma)}(1 + O(\pi^{p+1}))$. We must have $\sigma(a) \equiv a^{\omega(\sigma)} \pmod{\pi^{p+1}}$. This implies that

$$(1 + c\omega(\sigma)\pi^e + O(\pi^{e+1})) \equiv (1 + c\omega(\sigma)^e\pi^e + O(\pi^{e+1})) \pmod{\pi^{p+1}}.$$

Let's show that $e \geq p$. If $e < p$, we will have that $\omega(\sigma)^e = \omega(\sigma)$, for every $\sigma \in G$, in other words, for every $\omega(\sigma) \in (\mathbb{Z}/p\mathbb{Z})^*$. This would also imply that $e \equiv 1 \pmod{p-1}$, so $e = 1$. But since $e \geq 2$, we will have a contradiction. Hence, $e \geq p$.

So we have seen that every element $a \in U_1$ such that $\overline{a} \in B$ can be written as

$$a = \zeta_p^b(1 + c\pi^p + O(\pi^{p+1}))$$

for some integers $b, c \in \mathbb{Z}$. Clearly $(1 + \pi^p)$ is a generator of $\{u \equiv 1 \pmod{\pi^p}\}$ modulo U_1^p. Therefore, we have that B lies in the subgroup of U_1/U_1^p generated by the classes of ζ_p and $(1 + \pi^p)$ modulo U_1^p , which is an abelian group of exponent p and 2 generators. Hence, we woul have that $B \subseteq (\mathbb{Z}/p\mathbb{Z})^2$, a clear contradiction with the fact that $B \cong (\mathbb{Z}/p\mathbb{Z})^3$.

□

Therefore, since no extension of $\mathbb{Q}_p$ has Galois group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^3$, our original cyclic field K lives in $\mathbb{Q}_p(\zeta_m)$, as we wanted to prove. □

Theorem 5.9. *Let $K/\mathbb{Q}_2$ be a cyclic extension of degree 2^r, for $r \geq 1$. Then there exists $m \geq 1$ such that $K \subseteq \mathbb{Q}_2(\zeta_m)$.*

Proof. Analogously to the previous theorem, we already know of two extensions of $\mathbb{Q}_2$ that have cyclic galois group of order 2^r and lie in a cyclotomic extension.

One of them is the unramified extension $L_1 = \mathbb{Q}_2(\zeta_{2^{2^r}-1})$. Since $L_2 = \mathbb{Q}_2(\zeta_{2^{r+2}})$ has Galois group isomorphic to

$$\mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^{r+2}})/\mathbb{Q}_2) \cong (\mathbb{Z}/2^{r+2}\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z},$$

it will have a subextension with Galois group over $\mathbb{Q}_2$ cyclic of degree 2^r. Consider $m = (2^{2^r} - 1)2^{r+2}$. We will show that $K \subseteq \mathbb{Q}_2(\zeta_m)$ by reduction to absurdity.

Suppose that K isn't contained in $\mathbb{Q}_2(\zeta_m) = L_1 \cdot L_2$. Then, since L_1 is unramified and L_2 is totally ramified, they will be linearly disjoint and their compositum has Galois group $\mathrm{Gal}(\mathbb{Q}_2(\zeta_m)/\mathbb{Q}_2) \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^r\mathbb{Z})^2$. Hence,

$$\mathrm{Gal}(K(\zeta_m)/\mathbb{Q}_2) \hookrightarrow \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^r\mathbb{Z})^3.$$

We also know that $\mathrm{Gal}(K(\zeta_m)/\mathbb{Q}_2(\zeta_m)) \cong \mathbb{Z}/2^s\mathbb{Z}$, for some $1 < s \leq r$, and has as a quotient

$$\mathrm{Gal}(\mathbb{Q}_2(\zeta_m)/\mathbb{Q}_2) = \frac{\mathrm{Gal}(K(\zeta_m)/\mathbb{Q}_2)}{\mathrm{Gal}(K(\zeta_m)/\mathbb{Q}_2(\zeta_m))} \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^r\mathbb{Z})^2.$$

Therefore, we have two choices for the Galois group of $K(\zeta_m)$:

$$\mathrm{Gal}(K(\zeta_m)/\mathbb{Q}_2) = \begin{cases} \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^r\mathbb{Z})^2 \times (\mathbb{Z}/2^s\mathbb{Z}) & \text{with } s > 1. \\ (\mathbb{Z}/2^r\mathbb{Z})^2 \times (\mathbb{Z}/2^t\mathbb{Z}) & \text{with } r \geq t \geq 2. \end{cases}$$

In the second case we have $r \geq t > s$, and since $s \geq 1$, we can take $t \geq 2$.

In this situation, we will have a subfield N with

$$\mathrm{Gal}(N/\mathbb{Q}_2) = \begin{cases} (\mathbb{Z}/2\mathbb{Z})^4. \\ \text{or} \\ (\mathbb{Z}/4\mathbb{Z})^3. \end{cases}$$

We will see that this is not possible for either case. Since $\zeta_2 = -1 \in \mathbb{Q}_2$, we can apply Kummer theory to the abelian extensions of $\mathbb{Q}_2$. So we have that every extension of $\mathbb{Q}_2$ with finite abelian Galois group of exponent 2 will have a corresponding subgroup $A \subseteq \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ isomorphic to its Galois group. In particular, if the first possibility for N holds, there will be a subgroup A isomomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$. However, we saw in chapter 2 that $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \cong (\mathbb{Z}/2\mathbb{Z})^3$. So the first possibility is ruled out.

Lemma 5.10. *No extension $N/\mathbb{Q}_2$ has Galois group isomorphic to $(\mathbb{Z}/4\mathbb{Z})^3$.*

Proof. Suppose the contrary, that there exists some $N/\mathbb{Q}_2$ with Galois group isomomorphic to $(\mathbb{Z}/4\mathbb{Z})^3$. If $i \notin N$, then $[N(i) : N] = 2$ and

$$\mathrm{Gal}(N(i)/\mathbb{Q}_2) \cong (\mathbb{Z}/4\mathbb{Z})^3 \times \mathbb{Z}/2\mathbb{Z}.$$

Then we would have a subextension with Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$, which we have just shown to be impossible. So $i \in N$. We will have

$$\mathrm{Gal}(N/\mathbb{Q}_2(i)) \cong (\mathbb{Z}/4\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z},$$

and so it has a subgroup H isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2$. Therefore, if we define $L = N^H$, we will have $\mathrm{Gal}(L/\mathbb{Q}_2) \cong \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Q}_2(i) \subseteq L$.

Let σ be a generator of $\mathrm{Gal}(L/\mathbb{Q}_2)$. Then σ^2 generates $\mathrm{Gal}(L/\mathbb{Q}_2(i))$ and so

$$\sigma(i) = -i.$$

Since $[L : \mathbb{Q}_2(i)] = 2$, there exists some $a \in \mathbb{Q}_2(i)$ such that $L = \mathbb{Q}_2(i, \alpha)$, where $\alpha^2 = a$.

We have that

$$(\sigma^2(\alpha))^2 = \sigma^2(\alpha^2) = \alpha^2.$$

But since $\alpha \notin \mathbb{Q}_2(i)$, $\sigma^2(\alpha) \neq \alpha$. Hence, we will have $\sigma^2(\alpha) = -\alpha$. This also implies $\sigma^3(\alpha) = -\sigma(\alpha)$.

Therefore,

$$\sigma^2\left(\frac{\sigma(\alpha)}{\alpha}\right) = \frac{\sigma^3(\alpha)}{\sigma^2(\alpha)} = \frac{\sigma(\alpha)}{\alpha}.$$

Hence, we will have $\sigma(\alpha)/\alpha = x + iy \in \mathbb{Q}_2(i)$, with $x, y \in \mathbb{Q}_2$. On the other hand,

$$\sigma\left(\frac{\sigma(\alpha)}{\alpha}\right) = \sigma(x + iy) = x - iy.$$

Combining this we get

$$-1 = \frac{\sigma^2(\alpha)}{\alpha} = \frac{\sigma^2(\alpha)}{\sigma(\alpha)} \cdot \frac{\sigma(\alpha)}{\alpha} = (x+iy)(x-iy) = x^2 + y^2.$$

However, $x^2 + y^2 = -1$ has no solution in $\mathbb{Q}_2$. If it did, we could rewrite it as $x^2 + y^2 + 1 = 0$, and multiplying by suitable elements in $\mathbb{Z}_2$, we would get

$$A^2 + B^2 + C^2 = 0, \ A, B, C \in \mathbb{Z}_2.$$

Now, we can extract the common powers of 2 to assure that at least one the terms isn't divisible by 2, i.e. one of them will be different from 0 in $\mathbb{Z}_2/2\mathbb{Z}_2 \cong \mathbb{Z}/2\mathbb{Z}$. We also know that $a \in \mathbb{Z}_2^*$ is a square if and only if $a \equiv 1 \pmod{2^3}$. Then, we get:

$$A^2 + B^2 + C^2 \equiv 1, 2, \text{ or } 3 \pmod{2^3}.$$

With this we see that there are no solutions to the equation in $\mathbb{Q}_2$, so we have arrived at a contradiction. □

In conclusion, our original field K will be contained in $\mathbb{Q}_2(\zeta_m)$.

□

References

[Sut17] Andrew Sutherland. *18.785 Number Theory I*. Massachusetts Institute of Technology: MIT OpenCourseWare, avaliable at. Fall 2017.

[Que11] Jordi Quer. *Apunts de Teoria de Nombres, nombres p-àdics*. Curs 2010-2011.

[Gre74] M. J. Greenberg. "An Elementary Proof of the Kronecker-Weber Theorem". In: *The American Mathematical Monthly* 81.6 (1974), pp. 601–607. ISSN: 00029890, 19300972.

[Ser79] Jean-Pierre Serre. *Local Fields*. Graduate Texts in Mathematics. Springer-Verlag New York, 1979. ISBN: 978-0-387-90424-5.

[Gou93] Fernando Q. Gouvêa. *p-adic Numbers*. Universitext. Springer-Verlag Berlin Heidelberg, 1993. ISBN: 0-387-56844-1.

[Was97] Lawrence C. Washington. *Introduction to Cyclotomic Extensions*. Graduate Texts in Mathematics. Springer-Verlag New York, 1997. ISBN: 978-1-4612-1934-7.

[Sch98] Norbert Schappacher. "On the History of Hilbert's Twelfth Problem A Comedy of Errors". In: 3 (Jan. 1998).

[Rob00] Alain M. Robert. *A Course in p-adic analysis*. Graduate Texts in Mathematics. Springer-Verlag New York, 2000. ISBN: 978-0-387-98669-2.

[Ste04] William Stein. *A Brief Introduction to Classical and Adelic Algebraic Number Theory*. 2004.

[Mil17a] James S. Milne. *Algebraic Number Theory (v3.07)*. Available at. 2017, p. 165.

[Mil17b] James S. Milne. *Fields and Galois Theory (v4.53)*. Available at. 2017, p. 138.